SheppardMullin

GDPR AND U.S. STATES' GENERAL PRIVACY LAWS DESKBOOK

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

California Consumer Privacy Act of 2018

(as amended by the California Privacy Rights Act of 2020)

and Related Regulations

1798.100 General Duties of Businesses that Collect Personal Information[1]

(a) A business that controls the collection of a consumer's personal information shall, at or before the point of collection, inform consumers of the following:

(1) The categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether that information is sold or shared. A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected without providing the consumer with notice consistent with this section.

(2) If the business collects sensitive personal information, the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used, and whether that information is sold or shared. A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected without providing the consumer with notice consistent with this section.

(3) The length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine that period provided that a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose.

(b) A business that, acting as a third party, controls the collection of personal information about a consumer may satisfy its obligation under subdivision (a) by providing the required information prominently and conspicuously on the homepage of its internet website. In addition, if a business acting as a third party controls the collection of personal information about a consumer on its premises, including in a vehicle, then the business shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information are used, and whether that personal information is sold, in a clear and conspicuous manner at the location.

(c) A business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.

(d) A business that collects a consumer's personal information and that sells that personal information to, or shares it with, a third party or that discloses it to a service provider or contractor for a business purpose shall enter into an agreement with the third party, service provider, or contractor, that:

(1) Specifies that the personal information is sold or disclosed by the business only for limited and specified purposes.

(2) Obligates the third party, service provider, or contractor to comply with applicable obligations under this title and obligate those persons to provide the same level of privacy protection as is required by this title.

(3) Grants the business rights to take reasonable and appropriate steps to help ensure that the third party, service provider, or contractor uses the personal information transferred in a manner consistent with the business' obligations under this title.

[1] Bolded items in this section represent additions to the CCPA by the CPRA. Strike-thoughs represent content CPRA has removed from CCPA.

(4) Requires the third party, service provider, or contractor to notify the business if it makes a determination that it can no longer meet its obligations under this title.

(5) Grants the business the right, upon notice, including under paragraph (4), to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

(e) A business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Section 1798.81.5.

(f) Nothing in this section shall require a business to disclose trade secrets, as specified in regulations adopted pursuant to paragraph (3) of subdivision (a) of Section 1798.185.

1798.105 Consumers' Right to Delete Personal Information

(a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's rights to request the deletion of the consumer's personal information.

(c)

(1) A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records, notify any service providers or contractors to delete the consumer's personal information from their records, and notify all third parties to whom the business has sold or shared the personal information to delete the consumer's personal information unless this proves impossible or involves disproportionate effort.

(2) The business may maintain a confidential record of deletion requests solely for the purpose of preventing the personal information of a consumer who has submitted a deletion request from being sold, for compliance with laws or for other purposes, solely to the extent permissible under this title.

(3) A service provider or contractor shall cooperate with the business in responding to a verifiable consumer request, and at the direction of the business, shall delete, or enable the business to delete and shall notify any of its own service providers or contractors to delete personal information about the consumer collected, used, processed, or retained by the service provider or the contractor. The service provider or contractor shall notify any service providers, contractors, or third parties who may have accessed personal information from or through the service provider or contractor, unless the information was accessed at the direction of the business, to delete the consumer's personal information unless this proves impossible or involves disproportionate effort. A service provider or contractor shall not be required to comply with a deletion request submitted by the consumer directly to the service provider or contractor to the extent that the service provider or contractor has collected, used, processed, or retained the consumer's personal information in its role as a service provider or contractor to the business.

(d) A business, or a service provider, or contractor acting pursuant to its contract with the business , another service provider, or another contractor, shall not be required to comply with a consumer's request to delete the consumer's personal information if it is reasonably necessary for the business, ~~or~~ service provider, or contractor to maintain the consumer's personal information in order to:

(1) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated by the consumer within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

(3) Debug to identify and repair errors that impair existing intended functionality.

(4) Exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law.

(5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.

(6) Engage in public or peer-reviewed scientific, historical, or statistical research that conforms or adheres to all other applicable ethics and privacy laws, when the business' deletion of the information is likely to render impossible or seriously impair the ability to complete such research, if the consumer has provided informed consent.

(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business and compatible with the context in which the consumer provided the information.

(8) Comply with a legal obligation.

1798.106 Consumers' Right to Correct Inaccurate Personal Information

(a) A consumer shall have the right to request a business that maintains inaccurate personal information about the consumer to correct that inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the personal information.

(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's right to request correction of inaccurate personal information.

(c) A business that receives a verifiable consumer request to correct inaccurate personal information shall use commercially reasonable efforts to correct the inaccurate personal information as directed by the consumer, pursuant to Section 1798.130 and regulations adopted pursuant to paragraph (8) of subdivision (a) of Section 1798.185.

(Added November 3, 2020, by initiative Proposition 24, Sec. 6. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.110 Consumers' Right to Know What Personal Information is Being Collected. Right to Access Personal Information

(a) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following:

(1) The categories of personal information it has collected about that consumer.

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting, selling, or sharing personal information.

(4) The categories of third parties to whom the business discloses personal information.

(5) The specific pieces of personal information it has collected about that consumer.

(b) A business that collects personal information about a consumer shall disclose to the consumer, pursuant to subparagraph (B) of paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable consumer request from the consumer, provided that a business shall be deemed to be in compliance with paragraphs (1) to (4), inclusive, of subdivision (a) to the extent that the categories of information and the business or

commercial purpose for collecting, selling, or sharing personal information it would be required to disclose to the consumer pursuant to paragraphs (1) to (4), inclusive, of subdivision (a) is the same as the information it has disclosed pursuant to paragraphs (1) to (4), inclusive, of subdivision (c).

(c) A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The categories of personal information it has collected about consumers.

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting, selling, or sharing personal information.

(4) The categories of third parties to whom the business discloses personal information.

(5) That a consumer has the right to request the specific pieces of personal information the business has collected about that consumer.

1798.115 Consumers' Right to Know What Personal Information is Sold or Shared and to Whom

(a) A consumer shall have the right to request that a business that sells or shares the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer:

(1) The categories of personal information that the business collected about the consumer.

(2) The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold or shared, by category or categories of personal information for each category of third parties to whom the personal information was sold or shared.

(3) The categories of personal information that the business disclosed about the consumer for a business purpose and the categories of persons to whom it was disclosed for a business purpose.

(b) A business that sells or shares personal information about a consumer, or that discloses a consumer's personal information for a business purpose, shall disclose, pursuant to paragraph (4) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) to the consumer upon receipt of a verifiable consumer request from the consumer.

(c) A business that sells or shares consumers' personal information, or that discloses consumers' personal information for a business purpose, shall disclose, pursuant to subparagraph (C) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The category or categories of consumers' personal information it has sold or shared, or if the business has not sold or shared consumers' personal information, it shall disclose that fact.

(2) The category or categories of consumers' personal information it has disclosed for a business purpose, or if the business has not disclosed consumers' personal information for a business purpose, it shall disclose that fact.

(d) A third party shall not sell or share personal information about a consumer that has been sold to, or shared with, the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120.

1798.120 Consumers' Right to Opt Out of Sale or Sharing of Personal Information

(a) A consumer shall have the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information. This right may be referred to as the right to opt-out of sale or sharing.

(b) A business that sells consumers' personal information to, or shares it with, third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold or shared and that consumers have the "right to opt-out" of the sale or sharing of their personal information.

(c) Notwithstanding subdivision (a), a business shall not sell or share the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale or sharing of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age.

(d) A business that has received direction from a consumer not to sell or share the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell or share the minor consumer's personal information shall be prohibited, pursuant to paragraph (4) of subdivision (c) of Section 1798.135, from selling or sharing the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides consent for the sale or sharing of the consumer's personal information.

1798.121 Consumers' Right to Limit Use and Disclosure of Sensitive Personal Information

(a) A consumer shall have the right, at any time, to direct a business that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services, to perform the services set forth in paragraphs (2), (4), (5), and (8) of subdivision (e) of Section 1798.140, and as authorized by regulations adopted pursuant to subparagraph (C) of paragraph (19) of subdivision (a) of Section 1798.185. A business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in this subdivision shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be used, or disclosed to a service provider or contractor, for additional, specified purposes and that consumers have the right to limit the use or disclosure of their sensitive personal information.

(b) A business that has received direction from a consumer not to use or disclose the consumer's sensitive personal information, except as authorized by subdivision (a), shall be prohibited, pursuant to paragraph (4) of subdivision (c) of Section 1798.135, from using or disclosing the consumer's sensitive personal information for any other purpose after its receipt of the consumer's direction unless the consumer subsequently provides consent for the use or disclosure of the consumer's sensitive personal information for additional purposes.

(c) A service provider or contractor that assists a business in performing the purposes authorized by subdivision (a) may not use the sensitive personal information after it has received instructions from the business and to the extent it has actual knowledge that the personal information is sensitive personal information for any other purpose. A service provider or contractor is only required to limit its use of sensitive personal information received pursuant to a written contract with the business in response to instructions from the business and only with respect to its relationship with that business.

(d) Sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to this section, as further defined in regulations adopted pursuant to subparagraph (C) of paragraph (19) of subdivision (a) of Section 1798.185, and shall be treated as personal information for purposes of all other sections of this act, including Section 1798.100.

1798.125 Consumers' Right of No Retaliation Following Opt Out or Exercise of Other Rights

(a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer.

(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(E) Retaliating against an employee, applicant for employment, or independent contractor, as defined in subparagraph (A) of paragraph (2) of subdivision (m) of Section 1798.145, for exercising their rights under this title.

(2) Nothing in this subdivision prohibits a business, pursuant to subdivision (b), from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.

(3) This subdivision does not prohibit a business from offering loyalty, rewards, premium features, discounts, or club card programs consistent with this title.

(b) (1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale or sharing of personal information, or the retention of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is reasonably related to the value provided to the business by the consumer's data.

(2) A business that offers any financial incentives pursuant to this subdivision, shall notify consumers of the financial incentives pursuant to Section 1798.1350.

(3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.1350 that clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time. If a consumer refuses to provide opt-in consent, then the business shall wait for at least 12 months before next requesting that the consumer provide opt-in consent, or as prescribed by regulations adopted pursuant to Section 1798.185.

(4) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

1798.130 Notice, Disclosure, Correction, and Deletion Requirements

(a) In order to comply with Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:

(1) (A) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, or requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively, including, at a minimum, a toll-free telephone number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, or for requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively.

(B) If the business maintains an internet website, make the internet website available to consumers to submit requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, or requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively.

(2) (A) Disclose and deliver the required information to a consumer free of charge, to correct inaccurate personal information, or delete a consumer's personal information, based on the consumer's request, within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business's duty to disclose and deliver the information, to correct inaccurate personal information, or to delete personal information within 45 days of receipt of the consumer's request. The time period to provide the required information, to correct inaccurate personal information, or to delete personal information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure of the required information shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, but shall not require the consumer to create an account with the business in order to make a verifiable consumer request provided that if the consumer, has an account with the business, the business may require the consumer to use that account to submit a verifiable consumer request.

(B) The disclosure of the required information shall cover the 12-month period preceding the business' receipt of the verifiable consumer request provided that, upon the adoption of a regulation pursuant to paragraph (9) of subdivision (a) of Section 1798.185, a consumer may request that the business disclose the required information beyond the 12-month period, and the business shall be required to provide that information unless doing so proves impossible or would involve a disproportionate effort. A consumer's right to request required information beyond the 12-month period, and a business's obligation to provide that information, shall only apply to personal information collected on or after January 1, 2022. Nothing in this subparagraph shall require a business to keep personal information for any length of time.

(3) (A) A business that receives a verifiable consumer request pursuant to Section 1798.110 or 1798.115 shall disclose any personal information it has collected about a consumer, directly or indirectly, including through or by a service provider or contractor, to the consumer. A service provider or contractor shall not be required to comply with a verifiable consumer request received directly from a consumer or a consumer's authorized agent, pursuant to Section 1798.110 or 1798.115, to the extent that the service provider or contractor has collected personal information about the consumer in its role as a service provider or contractor. A service provider or contractor shall provide assistance to a business with which it has a contractual relationship with respect to the business' response to a verifiable consumer request, including, but not limited to, by providing to the business the consumer's personal information in the service provider or contractor's possession, which the service provider or contractor obtained as a result of providing services to the business, and by correcting inaccurate information or by enabling the business to do the same. A service provider or contractor that collects personal information pursuant to a written contract with a business shall be required to assist the business through appropriate technical and organizational measures in complying with the requirements of subdivisions (d) to (f), inclusive, of Section 1798.100, taking into account the nature of the processing.

(B) For purposes of subdivision (b) of Section 1798.110:

(i) To identify the consumer, associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(ii) Identify by category or categories the personal information collected about the consumer for the applicable period of time by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected; the categories of sources from which the consumer's personal information was collected; the business or commercial purpose for collecting, selling, or sharing the consumer's personal information; and the categories of third parties to whom the business discloses the consumer's personal information.

(iii) Provide the specific pieces of personal information obtained from the consumer in a format that is easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format that may also be transmitted to another entity at the consumer's request without hindrance. "Specific pieces of information" do not include data generated to help ensure security and integrity or as prescribed by regulation. Personal information is not considered to have been disclosed by a business when a consumer instructs a business to transfer the consumer's personal information from one business to another in the context of switching services.

(4) For purposes of subdivision (b) of Section 1798.115:

(A) Identify the consumer and associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information of the consumer that the business sold or shared during the applicable period of time by reference to the enumerated category in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was sold or shared during the applicable period of time by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold or shared. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (C).

(C) Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose during the applicable period of time by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information, and provide the categories of persons to whom the consumer's personal information was disclosed for a business purpose during the applicable period of time by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information disclosed. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (B).

(5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its internet website, and update that information at least once every 12 months:

(A) A description of a consumer's rights pursuant to Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, and 1798.125 and two or more designated methods for submitting requests, except as provided in subparagraph (A) of paragraph (1) of subdivision (a).

(B) For purposes of subdivision (c) of Section 1798.110:

(i) A list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.

(ii) The categories of sources from which consumers' personal information is collected.

(iii) The business or commercial purpose for collecting, selling, or sharing consumers' personal information.

(iv) The categories of third parties to whom the business discloses consumers' personal information.

(C) For purposes of paragraphs (1) and (2) of subdivision (c) of Section 1798.115, two separate lists:

(i) A list of the categories of personal information it has sold or shared about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information sold, or if the business has not sold or shared consumers' personal information in the preceding 12 months, the business shall prominently disclose that fact in its privacy policy.

(ii) A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describes the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(6) Ensure that all individuals responsible for handling consumer inquiries about the business' privacy practices or the business's compliance with this title are informed of all requirements in Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.125, and this section, and how to direct consumers to exercise their rights under those sections.

(7) Use any personal information collected from the consumer in connection with the business's verification of the consumer's request solely for the purposes of verification and shall not further disclose the personal information, retain it longer than necessary for purposes of verification, or use it for unrelated purposes.

(b) A business is not obligated to provide the information required by Sections 1798.110 and 1798.115 to the same consumer more than twice in a 12-month period.

(c) The categories of personal information required to be disclosed pursuant to Sections 1798.100, 1798.110, and 1798.115 shall follow the definitions of personal information and sensitive personal information in Section 1798.140 by describing the categories of personal information using the specific terms set forth in subparagraphs (A) to (K), inclusive, of paragraph (1) of subdivision (v) of Section 1798.140 and by describing the categories of sensitive personal information using the specific terms set forth in paragraphs (1) to (9), inclusive, of subdivision (ae) of Section 1798.140.

1798.135 Methods of Limiting Sale, Sharing, and Use of Personal Information and Use of Sensitive Personal Information

(a) A business that sells or shares consumers' personal information or uses or discloses consumers' sensitive personal information for purposes other than those authorized by subdivision (a) of Section 1798.121 shall, in a form that is reasonably accessible to consumers:

(1) Provide a clear and conspicuous link on the business's internet homepages, titled "Do Not Sell or Share My Personal Information," to an internet web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale or sharing of the consumer's personal information.

(2) Provide a clear and conspicuous link on the business' internet homepages, titled "Limit the Use of My Sensitive Personal Information," that enables a consumer, or a person authorized by the consumer, to limit the use or disclosure of the consumer's sensitive personal information to those uses authorized by subdivision (a) of Section 1798.121.

(3) At the business' discretion, utilize a single, clearly labeled link on the business' internet homepages, in lieu of complying with paragraphs (1) and (2), if that link easily allows a consumer to opt out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information.

(4) In the event that a business responds to opt-out requests received pursuant to paragraph (1), (2), or (3) by informing the consumer of a charge for the use of any product or service, present the terms of any financial incentive offered pursuant to subdivision (b) of Section 1798.125 for the retention, use, sale, or sharing of the consumer's personal information.

(b) (1) A business shall not be required to comply with subdivision (a) if the business allows consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information through an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism, based on technical specifications set forth in regulations adopted pursuant to paragraph (20) of subdivision (a) of Section 1798.185, to the business indicating the consumer's intent to opt out of the business' sale or sharing of the consumer's personal information or to limit the use or disclosure of the consumer's sensitive personal information, or both.

(2) A business that allows consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information pursuant to paragraph (1) may provide a link to a web page that enables the consumer to consent to the business ignoring the opt-out preference signal with respect to that business' sale

or sharing of the consumer's personal information or the use of the consumer's sensitive personal information for additional purposes provided that:

(A) The consent web page also allows the consumer or a person authorized by the consumer to revoke the consent as easily as it is affirmatively provided.

(B) The link to the web page does not degrade the consumer's experience on the web page the consumer intends to visit and has a similar look, feel, and size relative to other links on the same web page.

(C) The consent web page complies with technical specifications set forth in regulations adopted pursuant to paragraph (20) of subdivision (a) of Section 1798.185.

(3) A business that complies with subdivision (a) is not required to comply with subdivision (b). For the purposes of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b).

(c) A business that is subject to this section shall:

(1) Not require a consumer to create an account or provide additional information beyond what is necessary in order to direct the business not to sell or share the consumer's personal information or to limit use or disclosure of the consumer's sensitive personal information.

(2) Include a description of a consumer's rights pursuant to Sections 1798.120 and 1798.121, along with a separate link to the "Do Not Sell or Share My Personal Information" internet web page and a separate link to the "Limit the Use of My Sensitive Personal Information" internet web page, if applicable, or a single link to both choices, or a statement that the business responds to and abides by opt-out preference signals sent by a platform, technology, or mechanism in accordance with subdivision (b), in: (A) Its online privacy policy or policies if the business has an online privacy policy or policies. (B) Any California-specific description of consumers' privacy rights.

(3) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Sections 1798.120, 1798.121, and this section and how to direct consumers to exercise their rights under those sections.

(4) For consumers who exercise their right to opt-out of the sale or sharing of their personal information or limit the use or disclosure of their sensitive personal information, refrain from selling or sharing the consumer's personal information or using or disclosing the consumer's sensitive personal information and wait for at least 12 months before requesting that the consumer authorize the sale or sharing of the consumer's personal information or the use and disclosure of the consumer's sensitive personal information for additional purposes, or as authorized by regulations.

(5) For consumers under 16 years of age who do not consent to the sale or sharing of their personal information, refrain from selling or sharing the personal information of the consumer under 16 years of age and wait for at least 12 months before requesting the consumer's consent again, or as authorized by regulations or until the consumer attains 16 years of age.

(6) Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request.

(d) Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.

(e) A consumer may authorize another person to opt-out of the sale or sharing of the consumer's personal information and to limit the use of the consumer's sensitive personal information on the consumer's behalf including through an opt-out preference signal, as defined in paragraph (1) of subdivision (b), indicating the consumer's intent to opt out, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General regardless of whether the business has elected to comply with

subdivision (a) or (b). For purposes of clarity, a business that elects to comply with subdivision (a) may respond to the consumer's opt-out consistent with Section 1798.125.

(f) If a business communicates a consumer's opt-out request to any person authorized by the business to collect personal information, the person shall thereafter only use that consumer's personal information for a business purpose specified by the business, or as otherwise permitted by this title, and shall be prohibited from:

(1) Selling or sharing the personal information.

(2) Retaining, using, or disclosing that consumer's personal information. (A) or any purpose other than for the specific purpose of performing the services offered to the business. (B) Outside of the direct business relationship between the person and the business. (C) For a commercial purpose other than providing the services to the business.

(g) A business that communicates a consumer's opt-out request to a person pursuant to subdivision (f) shall not be liable under this title if the person receiving the opt-out request violates the restrictions set forth in the title provided that, at the time of communicating the opt-out request, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation. Any provision of a contract or agreement of any kind that purports to waive or limit in any way this subdivision shall be void and unenforceable.

1798.140 Definitions

For purposes of this title:

(a) "Advertising and marketing" means a communication by a business or a person acting on the business' behalf in any medium intended to induce a consumer to obtain goods, services, or employment.

(b) "Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.

(c) "Biometric information" means an individual's physiological, biological or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that is used or is intended to be used singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(d) "Business" means:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys, sells, or shares, the personal information of 100,000 or more consumers or households.

(C) Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information.

(2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding

with the business and with whom the business shares consumers' personal information. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark that the average consumer would understand that two or more entities are commonly owned.

(3) A joint venture or partnership composed of businesses in which each business has at least a 40 percent interest. For purposes of this title, the joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that personal information in the possession of each business and disclosed to the joint venture or partnership shall not be shared with the other business.

(4) A person that does business in California, that is not covered by paragraph (1), (2), or (3), and that voluntarily certifies to the California Privacy Protection Agency that it is in compliance with, and agrees to be bound by, this title.

(e) "Business purpose" means the use of personal information for the business' operational purposes, or other notified purposes, or for the service provider or contractor's operational purposes, as defined by regulations adopted pursuant to paragraph (11) of subdivision (a) of Section 1798.185, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the purpose for which the personal information was collected or processed or for another purpose that is compatible with the context in which the personal information was collected. Business purposes are:

(1) Auditing related to a counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

(2) Helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes.

(3) Debugging to identify and repair errors that impair existing intended functionality.

(4) Short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction, including, but not limited to with the business.

(5) Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, analytic services, providing storage, or providing similar services on behalf of the business.

(6) Providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer provided that, for the purpose of advertising and marketing, a service provider or contractor shall not combine the personal information of opted-out consumers that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or persons or collects from its own interaction with consumers.

(7) Undertaking internal research for technological development and demonstration.

(8) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

(f) "Collects," "collected," or "collection" means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.

(g) "Commercial purposes" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction.

(h) "Consent" means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent.

(i) "Consumer" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

(j) (1) "Contractor" means a person to whom the business makes available a consumer's personal information for a business purpose, pursuant to a written contract with the business, provided that the contract:

(A) Prohibits the contractor from:

(i) Selling or sharing the personal information.

(ii) Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract, or as otherwise permitted by this title.

(iii) Retaining, using, or disclosing the information outside of the direct business relationship between the contractor and the business.

(iv) Combining the personal information that the contractor receives pursuant to a written contract with the business with personal information that it receives from or on behalf of another person or persons, or collects from its own interaction with the consumer, provided that the contractor may combine personal information to perform any business purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) and in regulations adopted by the California Privacy Protection Agency.

(B) Includes a certification made by the contractor that the contractor understands the restrictions in subparagraph (A) and will comply with them.

(C) Permits, subject to agreement with the contractor, the business to monitor the contractor's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.

(2) If a contractor engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the contractor engages another person to assist in processing personal information for that business purpose, it shall notify the business of that engagement, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph (1).

(k) "Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.

(l) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice, as further defined by regulation.

(m) "Deidentified" means information that cannot reasonably be used to infer information about, or otherwise be linked to a particular consumer, provided that the business that possesses the information:

(1) Takes reasonable measures to ensure that the information cannot be associated with a consumer or household.

(2) Publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision.

(3) Contractually obligates any recipients of the information to comply with all provisions of this subdivision.

(n) "Designated methods for submitting requests" means a mailing address, email address, internet web page, internet web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.

(o) "Device" means any physical object that is capable of connecting to the Internet, directly or indirectly, or to another device.

(p) "Homepage" means the introductory page of an internet website and any internet web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, "About," "Information," or settings page, and any other location that allows consumers to review the notices required by this title, including, but not limited to, before downloading the application.

(q) "Household" means a group, however identified, of consumers who cohabitate with one another at the same residential address and share use of common devices or services.

(r) "Infer" or "inference" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

(s) "Intentionally interacts" means when the consumer intends to interact with a person, or disclose personal information to a person, via one or more deliberate interactions, including visiting the person's website or purchasing a good or service from the person. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a person.

(t) "Nonpersonalized advertising" means advertising and marketing that is based solely on a consumer's personal information derived from the consumer's current interaction with the business with the exception of the consumer's precise geolocation.

(u) "Person" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

(v) (1) "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

(B) Any personal information described in subdivision (e) of Section 1798.80.

(C) Characteristics of protected classifications under California or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement.

Geolocation data.

(G) Audio, electronic, visual, thermal, olfactory, or similar information.

(H) Professional or employment-related information.

(I) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).

(J) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(K) Sensitive personal information.

(2) "Personal information" does not include publicly available information, or lawfully obtained, truthful information that is a matter of public concern. For purposes of this paragraph, "publicly available" means: information that is lawfully made available from federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge.

(3) "Personal information" does not include consumer information that is deidentified or aggregate consumer information.

(w) "Precise geolocation" means any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet, except as prescribed by regulations.

(x) "Probabilistic identifier" means the identification of a consumer or a consumer's device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.

(y) "Processing" means any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means.

(z) "Profiling" means any form of automated processing of personal information, as further defined by regulations pursuant to paragraph (16) of subdivision (a) of Section 1798.185, to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(aa) "Pseudonymize" or "Pseudonymization" means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

(ab) "Research" means scientific analysis, systematic study, and observation, including basic research or applied research that is designed to develop of contribute to public or scientific knowledge and that adheres or otherwise conforms to all other

applicable ethics and privacy laws, including, but not limited to, ~~or~~ studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business' service or device for other purposes shall be:

(1) Compatible with the business purpose for which the personal information was collected.

(2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, by a business.

(3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain, other than as needed to support the research.

(4) Subject to business processes that specifically prohibit reidentification of the information, other than as needed to support the research.

(5) Made subject to business processes to prevent inadvertent release of deidentified information.

(6) Protected from any reidentification attempts.

(7) Used solely for research purposes that are compatible with the context in which the personal information was collected.

(8) Subjected by the business conducting the research to additional security controls that limit access to the research data to only those individuals as are necessary to carry out the research purpose.

(ac) "Security and integrity" means the ability of:

(1) Networks or information systems to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information.

(2) Businesses to detect security incidents, resist malicious, deceptive, fraudulent, or illegal actions and to help prosecute those responsible for those actions.

(3) Businesses to ensure the physical safety of natural persons.

(ad) (1) "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration.

(2) For purposes of this title, a business does not sell personal information when:

(A) A consumer uses or directs the business to intentionally:

(i) Disclose personal information.

(B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information or limited the use of the consumer's sensitive personal information for the purposes of alerting persons that the consumer has opted out of the sale of the consumer's personal information or limited the use of the consumer's sensitive personal information.

(C) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business provided that information is used or shared consistently with this title. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with this title. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

(ae) "Sensitive personal information" means:

(1) Personal information that reveals:

(A) A consumer's social security, driver's license, state identification card, or passport number.

(B) A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

(C) A consumer's precise geolocation.

(D) A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership.

(E) The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.

(F) A consumer's genetic data.

(2) (A) The processing of biometric information for the purpose of uniquely identifying a consumer.

(B) Personal information collected and analyzed concerning a consumer's health.

(C) Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

(3) Sensitive personal information that is "publicly available" pursuant to paragraph (2) of subdivision (v) shall not be considered sensitive personal information or personal information.

(af) "Service" or "services" means work, labor, and services, including services furnished in connection with the sale or repair of goods.

(ag) (1) "Service provider" means a person that processes personal information on behalf of a business and that receives from or on behalf of the business consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the person from: (A) Selling or sharing the personal information. (B) Retaining, using, or disclosing the personal information for any purpose other than the business purposes specified in the contract for the business, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract with the business, or as otherwise permitted by this title. (C) Retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the business. (D) Combining the personal information that the service provider receives from, or on behalf of, the business with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that the service provider may combine personal information to perform any business purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) of this section and in regulations adopted by the California Privacy Protection Agency. The contract may, subject to agreement with the service provider, permit the business to monitor the service provider's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.

(2) If a service provider engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the service provider engages another person to assist in processing personal information for that business purpose, it shall notify the business of that engagement, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph (1).

(ah) (1) "Share," "shared," or "sharing" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising

for the benefit of a business in which no money is exchanged. (2) For purposes of this title, a business does not share personal information when:

(A) A consumer uses or directs the business to intentionally disclose personal information or intentionally interact with one or more third parties.

(B) The business uses or shares an identifier for a consumer who has opted out of the sharing of the consumer's personal information or limited the use of the consumer's sensitive personal information for the purposes of alerting persons that the consumer has opted out of the sharing of the consumer's personal information or limited the use of the consumer's sensitive personal information.

(C) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with this title. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with this title. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

(ai) "Third party" means a person who is not any of the following:

(1) The business with whom the consumer intentionally interacts and that collects personal information from the consumer as part of the consumer's current interaction with the business under this title.

(2) A service provider to the business.

(3) A contractor.

(aj) "Unique identifier" or "unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device that is linked to a consumer or family. For purposes of this subdivision, "family" means a custodial parent or guardian and any children under 18 years of age over which the parent or guardian has custody.

(ak) "Verifiable consumer request" means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, or by a person who has power of attorney or is acting as a conservator for the consumer, and that the business can verify, using commercially reasonable methods, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115, to delete personal information pursuant to Section 1798.105, or to correct inaccurate personal information pursuant to Section 1798.106, if the business cannot verify, pursuant to this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.

1798.145 Compliance & Exemptions

(a) The obligations imposed on businesses by this title shall not restrict a business' ability to:

(1) Comply with federal, state, or local laws or comply with a court order or subpoena to provide information.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities. Law enforcement agencies, including police and sheriff's departments, may direct a business pursuant to a law enforcement agency-approved investigation with an active case number not to delete a consumer's personal information, and, upon receipt of that direction, a business shall not delete the personal information for 90 days in order to allow the law enforcement agency to obtain a court-issued subpoena, order, or warrant to obtain a consumer's personal information. For good cause and only to the extent necessary for investigatory purposes, a law enforcement agency may direct a business not to delete the consumer's personal information for additional 90-day periods. A business that has received direction from a law enforcement agency not to delete the personal information of a consumer who has requested deletion of the consumer's personal information shall not use the consumer's personal information for any purpose other than retaining it to produce to law enforcement in response to a court-issued subpoena, order, or warrant unless the consumer's deletion request is subject to an exemption from deletion under this title.

(3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

(4) Cooperate with a government agency request for emergency access to a consumer's personal information if a natural person is at risk or danger of death or serious physical injury provided that:

(A) The request is approved by a high-ranking agency officer for emergency access to a consumer's personal information.

(B) The request is based on the agency's good faith determination that it has a lawful basis to access the information on a nonemergency basis.

(C) The agency agrees to petition a court for an appropriate order within three days and to destroy the information if that order is not granted.

(5) Exercise or defend legal claims.

(6) Collect, use, retain, sell, share, or disclose consumers' personal information that is deidentified or aggregate consumer information.

(7) Collect, sell, or share a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not prohibit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.

(b) The obligations imposed on businesses by Sections 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, and 1798.135, shall not apply where compliance by the business with the title would violate an evidentiary privilege under California law and shall not prevent a business from providing the personal information of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.

(c) (1) This title shall not apply to any of the following:

(A) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104- 191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).

(B) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section.

(C) Personal information collected as part of a clinical trial or other biomedical research study subject to, or conducted in accordance with, the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration, provided that the information is not sold or shared in a manner not permitted by this subparagraph, and, if it is inconsistent, that participants be informed of that use and provide consent.

(2) For purposes of this subdivision, the definitions of "medical information" and "provider of health care" in Section 56.05 shall apply and the definitions of "business associate," "covered entity," and "protected health information" in Section 160.103 of Title 45 of the Code of Federal Regulations shall apply.

(d) (1) This title shall not apply to an activity involving the collection, maintenance, disclosure, sale, communicate, or use of any personal information bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency as defined by subdivision (f) of Section 1681a of Title 15 of the United States Code, who provides information for use in a consumer report as defined in subdivision (d) of Section 1681a of Title 15 of the United States Code.

(2) Paragraph (1) shall apply only to the extent that such activity involving the collection, maintenance, disclosure, sale, communication, or use of such information by that agency, furnisher, or user is subject to regulation under the Fair Credit Reporting Act (Section 1681 et seq., Title 15 of the United States Code and the information is not collected, maintained, used, communicated, disclosed, or sold except as authorized by the Fair Credit Reporting Act.

(3) This subdivision shall not apply to Section 1798.150.

(e) This title shall not apply to personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code) or the federal Farm Credit Act of 1971 (as amended in 12 U.S.C. 2001-2279cc and implementing regulations, 12 C.F.R. 600, et seq.). This subdivision shall not apply to Section 1798.150.

(f) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.). This subdivision shall not apply to Section 1798.150.

(g) (1) Section 1798.120 shall not apply to vehicle information or ownership information retained or shared between a new motor vehicle dealer, as defined in Section 426 of the Vehicle Code, and the vehicle's manufacturer, as defined in Section 672 of the Vehicle Code, if the vehicle information or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall conducted pursuant to Sections 30118 to 30120, inclusive, of Title 49 of the United States Code, provided that the new motor vehicle dealer or vehicle manufacturer with which that vehicle information or ownership information is shared does not sell, share, or use that information for any other purpose.

(2) Section 1798.120 shall not apply to vessel information or ownership information retained or shared between a vessel dealer and the vessel's manufacturer, as defined in Section 651 of the Harbors and Navigation Code, if the vessel information or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vessel repair covered by a vessel warranty or a recall conducted pursuant to Section 4310 of Title 46 of the United States Code, provided that the vessel dealer or vessel manufacturer with which that vessel information or ownership information is shared does not sell, share, or use that information for any other purpose.

(3) For purposes of this subdivision:

(A) "Ownership information" means the name or names of the registered owner or owners and the contact information for the owner or owners.

(B) "Vehicle information" means the vehicle information number, make, model, year, and odometer reading.

(C) "Vessel dealer" means a person who is engaged, wholly or in part, in the business of selling or offering for sale, buying or taking in trade for the purpose of resale, or exchanging, any vessel or vessels, as defined in Section 651 of the Harbors and Navigation Code, and receives or expects to receive money, profit, or any other thing of value.

(D) "Vessel information" means the hull identification number, model, year, month and year of production, and information describing any of the following equipment as shipped, transferred, or sold from the place of manufacture, including all attached parts and accessories:

(i) An inboard engine.

(ii) An outboard engine. (iii) A stern drive unit. (iv) An inflatable personal floatation device approved under Section 160.076 of Title 46 of the Code of Federal Regulations.

(h) Notwithstanding a business' obligations to respond to and honor consumer rights requests pursuant to this title:

(1) A time period for a business to respond a consumer for any verifiable consumer request may be extended by up to a total of 90 days where necessary, taking into account the complexity and number of the requests. The business shall inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(2) If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay and at the latest within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business taking action and any rights the consumer may have to appeal the decision to the business.

(3) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that any verifiable consumer request is manifestly unfounded or excessive.

(i) (1) A business that discloses personal information to a service provider or contractor in compliance with this title shall not be liable under this title if the service provider or contractor receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider or contractor intends to commit such a violation. A service provider or contractor shall likewise not be liable under this title for the obligations of a business for which it provides services as set forth in this title provided that the service provider or contractor shall be liable for its own violations of this title.

(2) A business that discloses personal information of a consumer, with the exception of consumers who have exercised their right to opt out of the sale or sharing of their personal information, consumers who have limited the use or disclosure of their sensitive personal information, and minor consumers who have not opted in to the collection or sale of their personal information, to a third party pursuant to a written contract that requires the third party to provide the same level of protection of the consumer's rights under this title as provided by the business shall not be liable under this title if the third party receiving the personal information uses it in violation of the restrictions set forth in this title provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the third party intends to commit such a violation.

(j) This title shall not be construed to require a business service provider, or contractor to:

(1) Reidentify or otherwise link information that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

(2) Retain any personal information about a consumer if, in the ordinary course of business, that information about the consumer would not be retained. (3) Maintain information in identifiable, linkable, or associable form, or collect, obtain, retain, or access any data or technology, in order to be capable of linking or associating a verifiable consumer request with personal information.

(k) The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other natural persons. A verifiable consumer request for specific pieces of personal information pursuant to Section 1798.110, to delete a consumer's personal information pursuant to Section 1798.105, or to correct inaccurate personal information pursuant to Section 1798.106, shall not extend to personal information about the consumer that belongs to, or the business maintains on behalf of, another natural person. A business may rely on representations made in a verifiable consumer request as to rights with respect to personal information and is under no legal requirement to seek out other persons that may have or claim to have rights to personal information, and a business is under no legal obligation under this title or any other provision of law to take any action under this title in the event of a dispute between or among persons claiming rights to personal information in the business' possession.

(l) The rights afforded to consumers and the obligations imposed on any business under this title shall not apply to the extent that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article I of the California Constitution.

(m) (1) This title shall not apply to any of the following:

(A) Personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of, that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or an independent contractor of, that business.

(B) Personal information that is collected by a business that is emergency contact information of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of, that business to the extent that the personal information is collected and used solely within the context of having an emergency contact on file.

(C) Personal information that is necessary for the business to retain to administer benefits for another natural person relating to the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of, that business to the extent that the personal information is collected and used solely within the context of administering those benefits.

(2) For purposes of this subdivision:

(A) "Independent contractor" means a natural person who provides any service to a business pursuant to a written contract.

(B) "Director" means a natural person designated in the articles of incorporation as director, or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) "Medical staff member" means a licensed physician and surgeon, dentist, or podiatrist, licensed pursuant to Division 2 (commencing with Section 500) of the Business and Professions Code and a clinical psychologist as defined in Section 1316.5 of the Health and Safety Code.

(D) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, including a chief executive officer, president, secretary, or treasurer.

(E) "Owner" means a natural person who meets one of the following criteria:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) his subdivision shall not apply to subdivision (a) of Section 1798.100 or Section 1798.150.

(4) This subdivision shall become inoperative on January 1, 2023.

(n) (1) The obligations imposed on businesses by Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.121, 1798.130, and 1798.135 shall not apply to personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who acted or is acting as an employee, owner, director, officer, or independent contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit, or government agency.

(2) For purposes of this subdivision:

(A) "Independent contractor" means a natural person who provides any service to a business pursuant to a written contract.

(B) "Director" means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(D) "Owner" means a natural person who meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall become inoperative on January 1, 2023.

(o) (1) Sections 1798.105 and 1798.120 shall not apply to a commercial credit reporting agency's collection, processing, sale, or disclosure of business controller information to the extent the commercial credit reporting agency uses the business controller information solely to identify the relationship of a consumer to a business that the consumer owns or contact the consumer only in the consumer's role as the owner, director, officer, or management employee of the business.

(2) For the purposes of this subdivision:

(A) "Business controller information" means the name or names of the owner or owners, director, officer, or management employee of a business and the contact information, including a business title, for the owner or owners, director, officer, or management employee.

(B) "Commercial credit reporting agency" has the meaning set forth in subdivision (b) of Section 1785.42.

(C) "Owner" means a natural person that meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(D) "Director" means a natural person designated in the articles of incorporation of a business as director, or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(E) "Officer" means a natural person elected or appointed by the board of directors of a business to manage the daily operations of a corporation, including a chief executive officer, president, secretary, or treasurer.

(F) "Management employee" means a natural person whose name and contact information is reported to or collected by a commercial credit reporting agency as the primary manager of a business and used solely within the context of the natural person's role as the primary manager of the business.

(p) The obligations imposed on businesses in Sections 1798.105, 1798.106, 1798.110, and 1798.115 shall not apply to household data.

(q) (1) This title does not require a business to comply with a verifiable consumer request to delete a consumer's personal information under Section 1798.105 to the extent the verifiable consumer request applies to a student's grades, educational scores, or educational test results that the business holds on behalf of a local educational agency, as defined in subdivision (d) of Section 49073.1 of the Education Code, at which the student is currently enrolled. If a business does not comply with a request pursuant to this section, it shall notify the consumer that it is acting pursuant to this exception.

(2) This title does not require, in response to a request pursuant to Section 1798.110, that a business disclose on educational standardized assessment or educational assessment or a consumer's specific responses to the educational standardized assessment or educational assessment if consumer access, possession, or control would jeopardize the validity and reliability of that educational standardized assessment or educational assessment. If a business does not comply with a request pursuant to this section, it shall notify the consumer that it is acting pursuant to this exception.

(3) For purposes of this subdivision:

(A) "Educational standardized assessment or educational assessment" means a standardized or nonstandardized quiz, test, or other assessment used to evaluate students in or for entry to kindergarten and grades 1 to 12, inclusive, schools, postsecondary institutions, vocational programs, and postgraduate programs that are accredited by an accrediting agency or organization recognized by the State of California or the United States Department of Education, as well as certification and licensure examinations used to determine competency and eligibility to receive certification or licensure from a government agency or government certification body.

(B) "Jeopardize the validity and reliability of that educational standardized assessment or educational assessment" means releasing information that would provide an advantage to the consumer who has submitted a verifiable consumer request or to another natural person.

(r) Sections 1798.105 and 1798.120 shall not apply to a business' use, disclosure, or sale of particular pieces of a consumer's personal information if the consumer has consented to the business' use, disclosure, or sale of that information to produce a physical item, including a school yearbook containing the consumer's photograph if:

(1) The business has incurred significant expense in reliance on the consumer's consent.

(2) Compliance with the consumer's request to opt out of the sale of the consumer's personal information or to delete the consumer's personal information would not be commercially reasonable.

(3) The business complies with the consumer's request as soon as it is commercially reasonable to do so.

1798.146 Applicability of Title

(a) This title shall not apply to any of the following:

(1) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the federal Health Information Technology for Economic and Clinical Health Act, Title XIII of the federal American Recovery and Reinvestment Act of 2009 (Public Law 111-5).

(2) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains, uses, and discloses patient information in the same manner as medical information or protected health information as described in paragraph (1).

(3) A business associate of a covered entity governed by the privacy, security, and data breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the federal Health Information Technology for Economic and Clinical Health Act, Title XIII of the federal American Recovery and Reinvestment Act of 2009 (Public Law 111-5), to the extent that the business associate maintains, uses, and discloses patient information in the same manner as medical information or protected health information as described in paragraph (1).

(4) (A) Information that meets both of the following conditions:

(i) It is deidentified in accordance with the requirements for deidentification set forth in Section 164.514 of Part 164 of Title 45 of the Code of Federal Regulations.

(ii) It is derived from patient information that was originally collected, created, transmitted, or maintained by an entity regulated by the Health Insurance Portability and Accountability Act, the Confidentiality Of Medical Information Act, or the Federal Policy for the Protection of Human Subjects, also known as the Common Rule.

(B) Information that met the requirements of subparagraph (A) but is subsequently reidentified shall no longer be eligible for the exemption in this paragraph, and shall be subject to applicable federal and state data privacy and security laws, including, but not limited to, the Health Insurance Portability and Accountability Act, the Confidentiality Of Medical Information Act, and this title.

(5) Information that is collected, used, or disclosed in research, as defined in Section 164.501 of Title 45 of the Code of Federal Regulations, including, but not limited to, a clinical trial, and that is conducted in accordance with applicable ethics, confidentiality, privacy, and security rules of Part 164 of Title 45 of the Code of Federal Regulations, the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, good clinical practice guidelines issued by the International Council for Harmonisation, or human subject protection requirements of the United States Food and Drug Administration.

(b) For purposes of this section, all of the following shall apply:

(1) "Business associate" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(2) "Covered entity" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(3) "Identifiable private information" has the same meaning as defined in Section 46.102 of Title 45 of the Code of Federal Regulations.

(4) "Individually identifiable health information" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(5) "Medical information" has the same meaning as defined in Section 56.05.

(6) "Patient information" shall mean identifiable private information, protected health information, individually identifiable health information, or medical information.

(7) "Protected health information" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(8) "Provider of health care" has the same meaning as defined in Section 56.05.

(Added by Stats. 2020, Ch. 172, Sec. 2. (AB 713) Effective September 25, 2020.)

1798.148 Reidentification of Deidentified Information

(a) A business or other person shall not reidentify, or attempt to reidentify, information that has met the requirements of paragraph (4) of subdivision (a) of Section 1798.146, except for one or more of the following purposes:

(1) Treatment, payment, or health care operations conducted by a covered entity or business associate acting on behalf of, and at the written direction of, the covered entity. For purposes of this paragraph, "treatment," "payment," "health care operations," "covered entity," and "business associate" have the same meaning as defined in Section 164.501 of Title 45 of the Code of Federal Regulations.

(2) Public health activities or purposes as described in Section 164.512 of Title 45 of the Code of Federal Regulations.

(3) Research, as defined in Section 164.501 of Title 45 of the Code of Federal Regulations, that is conducted in accordance with Part 46 of Title 45 of the Code of Federal Regulations, the Federal Policy for the Protection of Human Subjects, also known as the Common Rule.

(4) Pursuant to a contract where the lawful holder of the deidentified information that met the requirements of paragraph (4) of subdivision (a) of Section 1798.146 expressly engages a person or entity to attempt to reidentify the deidentified information in order to conduct testing, analysis, or validation of deidentification, or related statistical techniques, if the contract bans any other use or disclosure of the reidentified information and requires the return or destruction of the information that was reidentified upon completion of the contract.

(5) If otherwise required by law.

(b) In accordance with paragraph (4) of subdivision (a) of Section 1798.146, information reidentified pursuant this section shall be subject to applicable federal and state data privacy and security laws including, but not limited to, the Health Insurance Portability and Accountability Act, the Confidentiality of Medical Information Act, and this title.

(c) Beginning January 1, 2021, any contract for the sale or license of deidentified information that has met the requirements of paragraph (4) of subdivision (a) of Section 1798.146, where one of the parties is a person residing or doing business in the state, shall include the following, or substantially similar, provisions:

(1) A statement that the deidentified information being sold or licensed includes deidentified patient information.

(2) A statement that reidentification, and attempted reidentification, of the deidentified information by the purchaser or licensee of the information is prohibited pursuant to this section.

(3) A requirement that, unless otherwise required by law, the purchaser or licensee of the deidentified information may not further disclose the deidentified information to any third party unless the third party is contractually bound by the same or stricter restrictions and conditions.

(d) For purposes of this section, "reidentify" means the process of reversal of deidentification techniques, including, but not limited to, the addition of specific pieces of information or data elements that can, individually or in combination, be used to uniquely identify an individual or usage of any statistical method, contrivance, computer software, or other means that have the effect of associating deidentified information with a specific identifiable individual.

(Added by Stats. 2020, Ch. 172, Sec. 3. (AB 713) Effective September 25, 2020.)

1798.150 Personal Information Security Breaches

(a) (1) Any consumer whose[2] nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, or whose email address in combination with a password or security question and answer that would permit access to the account is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

(2) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

(b) Actions pursuant to this section may be brought by a consumer if prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. The implementation and maintenance of reasonable security procedures and practices pursuant to Section 1798.81.5 following a breach does not constitute a cure with respect to that breach. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.

(c) The cause of action established by this section shall apply only to violations as defined in subdivision (a) and shall not be based on violations of any other section of this title.[3] Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution.

---

[2] SB-561, proposed February 22, 2019 would add here, before the word "nonencrypted", the following: "rights under this title are violated, or whose".

[3] SB-561, proposed February 22, 2019, would remove the first sentence.

1798.155 Administrative Enforcement

(a) Any business, service provider, contractor, or other person that violates this title shall be liable for an administrative fine of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation or violations involving the personal information of consumers whom the business, service provider, contractor, or other person has actual knowledge are under 16 years of age, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185, in an administrative enforcement action brought by the California Privacy Protection Agency.

(b) Any administrative fine assessed for a violation of this title, and the proceeds of any settlement of an action brought pursuant to subdivision (~~b~~a), shall be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.160 with the intent to fully offset any costs incurred by the state courts the Attorney General, and the California Privacy Protection Agency in connection with this title.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 17. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.160 Consumer Privacy Fund

(a) A special fund to be known as the "Consumer Privacy Fund" is hereby created within the General Fund in the State Treasury, and is available upon appropriation by the Legislature first to offset any costs incurred by the state courts in connection with actions brought to enforce this title, the costs incurred by the Attorney General in carrying out the Attorney General's duties under this title, and then for the purposes of establishing an investment fund in the State Treasury, with any earnings or interest from the fund to be deposited in the General Fund, and making grants to promote and protect consumer privacy, educate children in the area of online privacy, and fund cooperative programs with international law enforcement organizations to combat fraudulent activities with respect to consumer data breaches.

(b) Funds transferred to the Consumer Privacy Fund shall be used exclusively as follows:

(1) To offset any costs incurred by the state courts and the Attorney General in connection with this title.

(2) After satisfying the obligations under paragraph (1), the remaining funds shall be allocated each fiscal year as follows:

(A) Ninety-one percent shall be invested by the Treasurer in financial assets with the goal of maximizing long term yields consistent with a prudent level of risk. The principal shall not be subject to transfer or appropriation, provided that any interest and earnings shall be transferred on an annual basis to the General Fund for appropriation by the Legislature for General Fund purposes.

(B) Nine percent shall be made available to the California Privacy Protection Agency for the purposes of making grants in California, with 3 percent allocated to each of the following grant recipients:

(i) Nonprofit organizations to promote and protect consumer privacy.

(ii) Nonprofit organizations and public agencies, including school districts, to educate children in the area of online privacy.

(iii) State and local law enforcement agencies to fund cooperative programs with international law enforcement organizations to combat fraudulent activities with respect to consumer data breaches.

(c) Funds in the Consumer Privacy Fund shall not be subject to appropriation or transfer by the Legislature for any other purpose.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 18. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.175 Conflicting Provisions

This title is intended to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information, including, but not limited to, Chapter 22 (commencing with Section 22575) of Division 8 of the Business and Professions Code and Title 1.81 (commencing with Section 1798.80). The provisions of this title are not limited to information collected electronically or over the Internet, but apply to the collection and sale of all personal information collected by a business from consumers. Wherever possible, law relating to consumers' personal information should be construed to harmonize with the provisions of this title, but in the event of a conflict between other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 19. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.180 Preemption

This title is a matter of statewide concern and supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection and sale of consumers' personal information by a business.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 20. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.185 Regulations

(a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas:

(1) Updating or adding categories of personal information to those enumerated in subdivision (c) of Section 1798.130 and subdivision (ev) of Section 1798.140, and updating or adding categories of sensitive personal information to those enumerated in subdivision (ae) of Section 1798.140 in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.

(2) Updating as needed the definitions of "deidentified" and "unique identifier" to address changes in technology, data collection, obstacles to implementation, and privacy concerns, and adding, modifying, or deleting categories to the definition of designated methods for submitting requests to facilitate a consumer's ability to obtain information from a business pursuant to Section 1798.130. The authority to update the definition of "deidentified" shall not apply to deidentification standards set forth in Section 164.514 of Title 45 of the Code of Federal Regulations, where such information previously was "protected health information" as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter, with the intention that trade secrets should not be disclosed in response to a verifiable consumer request.

(4) Establishing rules and procedures for the following:

(A) To facilitate and govern the submission of a request by a consumer to opt-out of the sale or sharing of personal information pursuant to Section 1798.12045 and to limit the use of a consumer's sensitive personal information pursuant to Section 1798.121 to ensure that consumers have the ability to exercise their choices without undue burden and to prevent business from engaging in deceptive or harassing conduct, including in retaliation against consumers for exercising their rights, while allowing businesses to inform consumers of the consequences of their decision to opt out of the sale or sharing of their personal information or to limit the use of their sensitive personal information.

(B) To govern business compliance with a consumer's opt-out request.

(C) For the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

(5) Adjusting the monetary thresholds in January of every odd-numbered year to reflect any increase in the Consumer Price Index, in: subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.140; subparagraph (A) of paragraph (1) of subdivision (a) of Section 1798.150; subdivision (a) of Section 1798.155; Section 1798.199.25; and subdivision (a) of Section 1798.199.90.

(6) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentives, within one year of passage of this title and as needed thereafter.

(7) Establishing rules and procedures to further the purposes of Sections 1798. 105, 1798.106, 1798.110 and 1798.115 and to facilitate a consumer's or the consumer's authorized agent's ability to delete personal information, correct inaccurate personal information pursuant to Section 1798.106, or obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business's determination that a request for information received ~~by~~ from a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business's authentication of the consumer's identity, within one year of passage of this title and as needed thereafter.

(8) Establishing how often, and under what circumstances, a consumer may request a correction pursuant to Section 1798.106, including standards governing the following: (A) How a business responds to a request for correction, including exceptions for requests to which a response is impossible or would involve disproportionate effort, and requests for correction of accurate information. (B) How concerns regarding the accuracy of the information may be resolved. (C) The steps a business may take to prevent fraud. (D) If a business rejects a request to correct personal information collected and analyzed concerning a consumer's health, the right of a consumer to provide a written addendum to the business with respect to any item or statement regarding any such personal information that the consumer believes to be incomplete or incorrect. The addendum shall be limited to 250 words per alleged incomplete or incorrect item and shall clearly indicate in writing that the consumer requests the addendum to be made a part of the consumer's record.

(9) Establishing the standard to govern a business' determination, pursuant to subparagraph (B) of paragraph (2) of subdivision (a) of Section 1798.130, that providing information beyond the 12-month period in a response to a verifiable consumer request is impossible or would involve a disproportionate effort.

(10) Issuing regulations further defining and adding to the business purposes, including other notified purposes, for which businesses, service providers, and contractors may use consumers' personal information consistent with consumers' expectations, and further defining the business purposes for which service providers and contractors may combine consumers' personal information obtained from different sources, except as provided for in paragraph (6) of subdivision (e) of Section 1798.140.

(11) Issuing regulations identifying those business purposes, including other notified purposes, for which service providers and contractors may use consumers' personal information received pursuant to a written contract with a business, for the service provider or contractor's own business purposes, with the goal of maximizing consumer privacy.

(12) Issuing regulations to further define "intentionally interacts," with the goal of maximizing consumer privacy.

(13) Issuing regulations to further define "precise geolocation," including if the size defined is not sufficient to protect consumer privacy in sparsely populated areas or when the personal information is used for normal operational purposes, including billing.

(14) Issuing regulations to define the term "specific pieces of information obtained from the consumer" with the goal of maximizing a consumer's right to access relevant personal information while minimizing the delivery of information to a consumer that would not be useful to the consumer, including system log information and other technical data. For delivery of the most sensitive personal information, the regulations may require a higher standard of authentication provided that the agency shall monitor the impact of the higher standard on the right of consumers to obtain their personal information to ensure that the requirements of verification do not result in the unreasonable denial of verifiable consumer requests.

(15) Issuing regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to:

(A) Perform a cybersecurity audit on an annual basis, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent. The factors to be considered in determining when processing may result in significant risk to the security of personal information shall include the size and complexity of the business and the nature and scope of processing activities.

(B) Submit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public. Nothing in this section shall require a business to divulge trade secrets.

(16) Issuing regulations governing access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer.

(17) Issuing regulations to further define a "law enforcement agency-approved investigation" for purposes of the exception in paragraph (2) of subdivision (a) of Section 1798.145.

(18) Issuing regulations to define the scope and process for the exercise of the agency's audit authority, to establish criteria for selection of persons to audit, and to protect consumers' personal information from disclosure to an auditor in the absence of a court order, warrant, or subpoena.

(19) (A) Issuing regulations to define the requirements and technical specifications for an opt-out preference signal sent by a platform, technology, or mechanism, to indicate a consumer's intent to opt out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information. The requirements and specifications for the opt-out preference signal should be updated from time to time to reflect the means by which consumers interact with businesses, and should:

(i) Ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business.

(ii) Ensure that the opt-out preference signal is consumer-friendly, clearly described, and easy to use by an average consumer and does not require that the consumer provide additional information beyond what is necessary.

(iii) Clearly represent a consumer's intent and be free of defaults constraining or presupposing that intent.

(iv) Ensure that the opt-out preference signal does not conflict with other commonly used privacy settings or tools that consumers may employ.

(v) Provide a mechanism for the consumer to selectively consent to a business' sale of the consumer's personal information, or the use or disclosure of the consumer's sensitive personal information, without affecting the consumer's preferences with respect to other businesses or disabling the opt-out preference signal globally.

(vi) State that in the case of a page or setting view that the consumer accesses to set the opt-out preference signal, the consumer should see up to three choices, including:

(I) Global opt out from sale and sharing of personal information, including a direction to limit the use of sensitive personal information.

(II) Choice to "Limit the Use of My Sensitive Personal Information."

(III) Choice titled "Do Not Sell/Do Not Share My Personal Information for Cross-Context Behavioral Advertising."

(B) Issuing regulations to establish technical specifications for an opt-out preference signal that allows the consumer, or the consumer's parent or guardian, to specify that the consumer is less than 13 years of age or at least 13 years of age and less than 16 years of age.

(C) Issuing regulations, with the goal of strengthening consumer privacy while considering the legitimate operational interests of businesses, to govern the use or disclosure of a consumer's sensitive personal information, notwithstanding the consumer's direction to limit the use or disclosure of the consumer's sensitive personal information, including:

(i) Determining any additional purposes for which a business may use or disclose a consumer's sensitive personal information.

(ii) Determining the scope of activities permitted under paragraph (8) of subdivision (e) of Section 1798.140, as authorized by subdivision (a) of Section 1798.121, to ensure that the activities do not involve health-related research.

(iii) Ensuring the functionality of the business' operations.

(iv) Ensuring that the exemption in subdivision (d) of Section 1798.121 for sensitive personal information applies to information that is collected or processed incidentally, or without the purpose of inferring characteristics about a consumer, while ensuring that businesses do not use the exemption for the purpose of evading consumers' rights to limit the use and disclosure of their sensitive personal information under Section 1798.121.

(20 Issuing regulations to govern how a business that has elected to comply with subdivision (b) of Section 1798.135 responds to the opt-out preference signal and provides consumers with the opportunity subsequently to consent to the sale or sharing of their personal information or the use and disclosure of their sensitive personal information for purposes in addition to those authorized by subdivision (a) of Section 1798.121. The regulations should:

(A) Strive to promote competition and consumer choice and be technology neutral.

(B) Ensure that the business does not respond to an opt-out preference signal by:

(i) Intentionally degrading the functionality of the consumer experience.

(ii) Charging the consumer a fee in response to the consumer's opt-out preferences.

(iii) Making any products or services not function properly or fully for the consumer, as compared to consumers who do not use the opt-out preference signal.

(iv) Attempting to coerce the consumer to opt in to the sale or sharing of the consumer's personal information, or the use or disclosure of the consumer's sensitive personal information, by stating or implying that the use of the opt-out preference signal will adversely affect the consumer as compared to consumers who do not use the opt-out preference signal, including stating or implying that the consumer will not be able to use the business' products or services or that those products or services may not function properly or fully.

(v) Displaying any notification or pop-up in response to the consumer's opt-out preference signal.

(C) Ensure that any link to a web page or its supporting content that allows the consumer to consent to opt in:

(i) Is not part of a popup, notice, banner, or other intrusive design that obscures any part of the web page the consumer intended to visit from full view or that interferes with or impedes in any way the consumer's experience visiting or browsing the web page or website the consumer intended to visit.

(ii) Does not require or imply that the consumer must click the link to receive full functionality of any products or services, including the website.

(iii) Does not make use of any dark patterns.

(iv) Applies only to the business with which the consumer intends to interact.

(D) Strive to curb coercive or deceptive practices in response to an opt-out preference signal but should not unduly restrict businesses that are trying in good faith to comply with Section 1798.135.

(21) Review existing Insurance Code provisions and regulations relating to consumer privacy, except those relating to insurance rates or pricing, to determine whether any provisions of the Insurance Code provide greater protection to consumers than the provisions of this title. Upon completing its review, the agency shall adopt a regulation that applies only the more protective provisions of this title to insurance companies. For the purpose of clarity, the Insurance Commissioner shall have jurisdiction over insurance rates and pricing.

(22) Harmonizing the regulations governing opt-out mechanisms, notices to consumers, and other operational mechanisms in this title to promote clarity and the functionality of this title for consumers.

(b) The Attorney General may adopt additional regulations as necessary to further the purposes of this title.

(c) The Attorney General shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner.

(d) Notwithstanding subdivision (a), the timeline for adopting final regulations required by the act adding this subdivision shall be July 1, 2022. Beginning the later of July 1, 2021, or six months after the agency provides notice to the Attorney General that it is prepared to begin rulemaking under this title, the authority assigned to the Attorney General to adopt regulations under this section shall be exercised by the California Privacy Protection Agency. Notwithstanding any other law, civil and administrative enforcement of the provisions of law added or amended by this act shall not commence until July 1, 2023, and shall only apply to violations occurring on or after that date. Enforcement of provisions of law contained in the California Consumer Privacy Act of 2018 amended by this act shall remain in effect and shall be enforceable until the same provisions of this act become enforceable.

1798.190 Anti-Avoidance

A court or the agency shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title:

(a) If a series of steps or transactions were component parts of a single transaction intended from the beginning to be taken with the intention of avoiding the reach of this title, including the disclosure of information by a business to a third party in order to avoid the definition of sell or share.

(b) If steps or transactions were taken to purposely avoid the definition of sell or share by eliminating any monetary or other valuable consideration, including by entering into contracts that do not include an exchange for monetary or other valuable consideration, but where a party is obtaining something of value or use.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 22. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.192 Waiver

Any provision of a contract or agreement of any kind, including a representative action waiver, that purports to waive or limit in any way rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable. This section shall not prevent a consumer from declining to request information from a business, declining to opt-out of a business's sale of the consumer's personal information, or authorizing a business to sell or share the consumer's personal information after previously opting out.

1798.194 Liberal Construction of Title

This title shall be liberally construed to effectuate its purposes.

(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.196 Relation to Federal and State Laws

This title is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the United States or California Constitution.

1798.198 Effective Date

(a) Subject to limitation provided in subdivision (b), and in Section 1798.199 this title shall be operative January 1, 2020.

(b) This title shall become operative only if initiative measure No. 17-0039, The Consumer Right to Privacy Act of 2018, is withdrawn from the ballot pursuant to Section 9604 of the Elections Code.

1798.199 Effective Date for Preemption

Notwithstanding Section 1798.198, Section 1798.180 shall be operative on the effective date of the act adding this section.

1798.199.10. Establishment of California Privacy Protection Agency

(a) There is hereby established in state government the California Privacy Protection Agency, which is vested with full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act of 2018. The agency shall be governed by a five-member board, including the chairperson. The chairperson and one member of the board shall be appointed by the Governor. The Attorney General, Senate Rules Committee, and Speaker of the Assembly shall each appoint one member. These appointments should be made from among Californians with expertise in the areas of privacy, technology, and consumer rights.

(b) The initial appointments to the agency shall be made within 90 days of the effective date of the act adding this section.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.1. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.15. Board Member Duties

Members of the agency board shall:

(a) Have qualifications, experience, and skills, in particular in the areas of privacy and technology, required to perform the duties of the agency and exercise its powers.

(b) Maintain the confidentiality of information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers, except to the extent that disclosure is required by the Public Records Act.

(c) Remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from another.

(d) Refrain from any action incompatible with their duties and engaging in any incompatible occupation, whether gainful or not, during their term.

(e) Have the right of access to all information made available by the agency to the chairperson.

(f) Be precluded, for a period of one year after leaving office, from accepting employment with a business that was subject to an enforcement action or civil action under this title during the member's tenure or during the five-year period preceding the member's appointment.

(g) Be precluded for a period of two years after leaving office from acting, for compensation, as an agent or attorney for, or otherwise representing, any other person in a matter pending before the agency if the purpose is to influence an action of the agency.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.2. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.20. Member Terms

Members of the agency board, including the chairperson, shall serve at the pleasure of their appointing authority but shall serve for no longer than eight consecutive years.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.3. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.25. Compensation

For each day on which they engage in official duties, members of the agency board shall be compensated at the rate of one hundred dollars ($100), adjusted biennially to reflect changes in the cost of living, and shall be reimbursed for expenses incurred in performance of their official duties.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.4. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.30. Executive Director; Officers, Counsel, Employees; Compensation

The agency board shall appoint an executive director who shall act in accordance with agency policies and regulations and with applicable law. The agency shall appoint and discharge officers, counsel, and employees, consistent with applicable civil service laws, and shall fix the compensation of employees and prescribe their duties. The agency may contract for services that cannot be provided by its employees.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.5. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.35. Delegation of Authority

The agency board may delegate authority to the chairperson or the executive director to act in the name of the agency between meetings of the agency, except with respect to resolution of enforcement actions and rulemaking authority.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.6. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.40. Agency Functions

The agency shall perform the following functions:

(a) Administer, implement, and enforce through administrative actions this title.

(b) On and after the later of July 1, 2021, or within six months of the agency providing the Attorney General with notice that it is prepared to assume rulemaking responsibilities under this title, adopt, amend, and rescind regulations pursuant to Section 1798.185 to carry out the purposes and provisions of the California Consumer Privacy Act of 2018, including regulations specifying recordkeeping requirements for businesses to ensure compliance with this title.

(c) Through the implementation of this title, protect the fundamental privacy rights of natural persons with respect to the use of their personal information, it is .

(d) Promote public awareness and understanding of the risks, rules, responsibilities, safeguards, and rights in relation to the collection, use, sale, and disclosure of personal information, including the rights of minors with respect to their own information, and provide a public report summarizing the risk assessments filed with the agency pursuant to paragraph (15) of subdivision (a) of Section 1798.185 while ensuring that data security is not compromised.

(e) Provide guidance to consumers regarding their rights under this title.

(f) Provide guidance to businesses regarding their duties and responsibilities under this title and appoint a Chief Privacy Auditor to conduct audits of businesses to ensure compliance with this title pursuant to regulations adopted pursuant to paragraph (18) of subdivision (a) of Section 1798.185.

(g) Provide technical assistance and advice to the Legislature, upon request, with respect to privacy-related legislation.

(h) Monitor relevant developments relating to the protection of personal information and, in particular, the development of information and communication technologies and commercial practices.

(i) Cooperate with other agencies with jurisdiction over privacy laws and with data processing authorities in California, other states, territories, and countries to ensure consistent application of privacy protections.

(j) Establish a mechanism pursuant to which persons doing business in California that do not meet the definition of business set forth in paragraph (1), (2), or (3) of subdivision (d) of Section 1798.140 may voluntarily certify that they are in compliance

with this title, as set forth in paragraph (4) of subdivision (d) of Section 1798.140, and make a list of those entities available to the public.

(k) Solicit, review, and approve applications for grants to the extent funds are available pursuant to paragraph (2) of subdivision (b) of Section 1798.160.

(l) Perform all other acts necessary or appropriate in the exercise of its power, authority, and jurisdiction and seek to balance the goals of strengthening consumer privacy while giving attention to the impact on businesses.

(Amended by Stats. 2021, Ch. 525, Sec. 5. (AB 694) Effective January 1, 2022.)

1798.199.45. Investigations

(a) Upon the sworn complaint of any person or on its own initiative, the agency may investigate possible violations of this title relating to any business, service provider, contractor, or person. The agency may decide not to investigate a complaint or decide to provide a business with a time period to cure the alleged violation. In making a decision not to investigate or provide more time to cure, the agency may consider the following:

(1) Lack of intent to violate this title.

(2) Voluntary efforts undertaken by the business, service provider, contractor, or person to cure the alleged violation prior to being notified by the agency of the complaint.

(b) The agency shall notify in writing the person who made the complaint of the action, if any, the agency has taken or plans to take on the complaint, together with the reasons for that action or nonaction.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.8. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.50. Due Process

No finding of probable cause to believe this title has been violated shall be made by the agency unless, at least 30 days prior to the agency's consideration of the alleged violation, the business, service provider, contractor, or person alleged to have violated this title is notified of the violation by service of process or registered mail with return receipt requested, provided with a summary of the evidence, and informed of their right to be present in person and represented by counsel at any proceeding of the agency held for the purpose of considering whether probable cause exists for believing the person violated this title. Notice to the alleged violator shall be deemed made on the date of service, the date the registered mail receipt is signed, or if the registered mail receipt is not signed, the date returned by the post office. A proceeding held for the purpose of considering probable cause shall be private unless the alleged violator files with the agency a written request that the proceeding be public.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.9. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.55. Hearings

(a) When the agency determines there is probable cause for believing this title has been violated, it shall hold a hearing to determine if a violation has or violations have occurred. Notice shall be given and the hearing conducted in accordance with the Administrative Procedure Act (Chapter 5 (commencing with Section 11500), Part 1, Division 3, Title 2, Government Code). The agency shall have all the powers granted by that chapter. If the agency determines on the basis of the hearing conducted pursuant to this subdivision that a violation or violations have occurred, it shall issue an order that may require the violator to do all or any of the following:

(1) Cease and desist violation of this title.

(2) Subject to Section 1798.155, pay an administrative fine of up to two thousand five hundred dollars ($2,500) for each violation, or up to seven thousand five hundred dollars ($7,500) for each intentional violation and each violation involving the personal information of minor consumers to the Consumer Privacy Fund within the General Fund of the state. When the agency determines that no violation has occurred, it shall publish a declaration so stating.

(b) If two or more persons are responsible for any violation or violations, they shall be jointly and severally liable.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.10. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.60. Rejection of ALJ Decision

Whenever the agency rejects the decision of an administrative law judge made pursuant to Section 11517 of the Government Code, the agency shall state the reasons in writing for rejecting the decision.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.11. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.65. Power of Subpoena; Power to Audit

The agency may subpoena witnesses, compel their attendance and testimony, administer oaths and affirmations, take evidence and require by subpoena the production of any books, papers, records, or other items material to the performance of the agency's duties or exercise of its powers, including, but not limited to, its power to audit a business' compliance with this title.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.12. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.70. Limitations

No administrative action brought pursuant to this title alleging a violation of any of the provisions of this title shall be commenced more than five years after the date on which the violation occurred.

(a) The service of the probable cause hearing notice, as required by Section 1798.199.50, upon the person alleged to have violated this title shall constitute the commencement of the administrative action.

(b) If the person alleged to have violated this title engages in the fraudulent concealment of the person's acts or identity, the five-year period shall be tolled for the period of the concealment. For purposes of this subdivision, "fraudulent concealment" means the person knows of material facts related to the person's duties under this title and knowingly conceals them in performing or omitting to perform those duties for the purpose of defrauding the public of information to which it is entitled under this title.

(c) If, upon being ordered by a superior court to produce any documents sought by a subpoena in any administrative proceeding under this title, the person alleged to have violated this title fails to produce documents in response to the order by the date ordered to comply therewith, the five-year period shall be tolled for the period of the delay from the date of filing of the motion to compel until the date the documents are produced.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.13. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.75. Civil Actions

(a) In addition to any other available remedies, the agency may bring a civil action and obtain a judgment in superior court for the purpose of collecting any unpaid administrative fines imposed pursuant to this title after exhaustion of judicial review of the agency's action. The action may be filed as a small claims, limited civil, or unlimited civil case depending on the jurisdictional amount. The venue for this action shall be in the county where the administrative fines were imposed by the agency. In order to obtain a judgment in a proceeding under this section, the agency shall show, following the procedures and rules of evidence as applied in ordinary civil actions, all of the following:

(1) That the administrative fines were imposed following the procedures set forth in this title and implementing regulations.

(2) That the defendant or defendants in the action were notified, by actual or constructive notice, of the imposition of the administrative fines.

(3) That a demand for payment has been made by the agency and full payment has not been received.

(b) A civil action brought pursuant to subdivision (a) shall be commenced within four years after the date on which the administrative fines were imposed.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.14. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.80. Application for Judgment to Collect Fines

(a) If the time for judicial review of a final agency order or decision has lapsed, or if all means of judicial review of the order or decision have been exhausted, the agency may apply to the clerk of the court for a judgment to collect the administrative fines imposed by the order or decision, or the order as modified in accordance with a decision on judicial review.

(b) The application, which shall include a certified copy of the order or decision, or the order as modified in accordance with a decision on judicial review, and proof of service of the order or decision, constitutes a sufficient showing to warrant issuance of the judgment to collect the administrative fines. The clerk of the court shall enter the judgment immediately in conformity with the application.

(c) An application made pursuant to this section shall be made to the clerk of the superior court in the county where the administrative fines were imposed by the agency.

(d) A judgment entered in accordance with this section has the same force and effect as, and is subject to all the provisions of law relating to, a judgment in a civil action and may be enforced in the same manner as any other judgment of the court in which it is entered.

(e) The agency may bring an application pursuant to this section only within four years after the date on which all means of judicial review of the order or decision have been exhausted.

(f) The remedy available under this section is in addition to those available under any other law.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.15. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.85. Judicial Review

Any decision of the agency with respect to a complaint or administrative fine shall be subject to judicial review in an action brought by an interested party to the complaint or administrative fine and shall be subject to an abuse of discretion standard.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.16. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.90. Violation; Penalties

(a) Any business, service provider, contractor, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation and each violation involving the personal information of minor consumers, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General. The court may consider the good faith cooperation of the business, service provider, contractor, or other person in determining the amount of the civil penalty.

(b) Any civil penalty recovered by an action brought by the Attorney General for a violation of this title, and the proceeds of any settlement of any said action, shall be deposited in the Consumer Privacy Fund.

(c) The agency shall, upon request by the Attorney General, stay an administrative action or investigation under this title to permit the Attorney General to proceed with an investigation or civil action and shall not pursue an administrative action or investigation, unless the Attorney General subsequently determines not to pursue an investigation or civil action. The agency may not limit the authority of the Attorney General to enforce this title.

(d) No civil action may be filed by the Attorney General under this section for any violation of this title after the agency has issued a decision pursuant to Section 1798.199.85 or an order pursuant to Section 1798.199.55 against that person for the same violation.

(e) This section shall not affect the private right of action provided for in Section 1798.150.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.17. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.95. Appropriations

(a) There is hereby appropriated from the General Fund of the state to the agency the sum of five million dollars ($5,000,000) during the fiscal year 2020–2021, and the sum of ten million dollars ($10,000,000) adjusted for cost-of-living changes, during each fiscal year thereafter, for expenditure to support the operations of the agency pursuant to this title. The expenditure of funds under this appropriation shall be subject to the normal administrative review given to other state appropriations. The Legislature shall appropriate those additional amounts to the commission and other agencies as may be necessary to carry out the provisions of this title.

(b) The Department of Finance, in preparing the state budget and the Budget Act bill submitted to the Legislature, shall include an item for the support of this title that shall indicate all of the following:

(1) The amounts to be appropriated to other agencies to carry out their duties under this title, which amounts shall be in augmentation of the support items of those agencies.

(2) The additional amounts required to be appropriated by the Legislature to the agency to carry out the purposes of this title, as provided for in this section.

(3) In parentheses, for informational purposes, the continuing appropriation during each fiscal year of ten million dollars ($10,000,000), adjusted for cost-of-living changes made pursuant to this section.

(c) The Attorney General shall provide staff support to the agency until the agency has hired its own staff. The Attorney General shall be reimbursed by the agency for these services.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.18. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.100. Considerations of Good Faith Cooperation

The agency and any court, as applicable, shall consider the good faith cooperation of the business, service provider, contractor, or other person in determining the amount of any administrative fine or civil penalty for a violation of this title. A business shall not be required by the agency, a court, or otherwise to pay both an administrative fine and a civil penalty for the same violation.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.19. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

California Consumer Privacy Act Regulations

Article 1. GENERAL PROVISIONS

11 C.F.R. § 7000. Title and Scope

(a) This Chapter shall be known as the California Consumer Privacy Act Regulations. It may be cited as such and will be referred to in this Chapter as "these regulations." These regulations govern compliance with the California Consumer Privacy Act and do not limit any other rights that consumers may have.

(b) A violation of these regulations shall constitute a violation of the CCPA and be subject to the remedies provided for therein.

Note: Authority cited: Sections 1798.175 and 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145, 1798.150, 1798.155, 1798.175, 1798.185, 1798.199.40, 1798.199.45, 1798.199.50, 1798.199.55 and 1798.199.65, Civil Code.

11 C.F.R. § 7001. Definitions.

In addition to the definitions set forth in Civil Code section 1798.140, for purposes of these regulations:

(a) "Agency" means the California Privacy Protection Agency established by Civil Code section 1798.199.10 et seq.

(b) "Alternative Opt-out Link" means the alternative opt-out link that a business may provide instead of posting the two separate "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links as set forth in Civil Code section 1798.135, subdivision (a)(3), and specified in section 7015.

(c) "Attorney General" means the California Attorney General or any officer or employee of the California Department of Justice acting under the authority of the California Attorney General.

(d) "Authorized agent" means a natural person or a business entity that a consumer has authorized to act on their behalf subject to the requirements set forth in section 7063.

(e) "Categories of sources" means types or groupings of persons or entities from which a business collects personal information about consumers, described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity. They may include the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.

(f) "Categories of third parties" means types or groupings of third parties with whom the business shares personal information, described with enough particularity to provide consumers with a meaningful understanding of the type of third party. They may include advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.

(g) "CCPA" means the California Consumer Privacy Act of 2018, Civil Code section 1798.100 et seq.

(h) "COPPA" means the Children's Online Privacy Protection Act, 15 U.S.C. sections 6501 to 6506 and 16 Code of Federal Regulations part 312.

(i) "Disproportionate effort" within the context of a business, service provider, contractor, or third party responding to a consumer request means the time and/or resources expended by the business, service provider, contractor, or third party to respond to the individualized request significantly outweighs the reasonably foreseeable impact to the consumer by not responding, taking into account applicable circumstances, such as the size of the business, service provider, contractor, or third party, the nature of the request, and the technical limitations impacting their ability to respond. For example, responding to a consumer request to know may require disproportionate effort when the personal information that is the subject of the request is not in a searchable or readily-accessible format, is maintained only for legal or compliance purposes, is not sold or used for any commercial purpose, and there is no reasonably foreseeable material impact to the consumer by not responding. By contrast, the impact to the consumer of denying a request to correct inaccurate information that the business uses and/or sells may outweigh the burden on the business, service provider, contractor, or third party in honoring the request when the reasonably foreseeable consequence of denying the request would be the denial of services or opportunities to the consumer. A business, service provider, contractor, or third party that has failed to put in place adequate processes and procedures to receive and process consumer requests in accordance with the CCPA and these regulations cannot claim that responding to a consumer's request requires disproportionate effort.

(j) "Employment benefits" means retirement, health, and other benefit programs, services, or products to which consumers and their dependents or their beneficiaries receive access through the consumer's employer.

(k) Employment-related information" means personal information that is collected by the business about a natural person for the reasons identified in Civil Code section 1798.145, subdivision (m)(1). The collection of employment-related information, including for the purpose of administering employment benefits, shall be considered a business purpose.

(l) "Financial incentive" means a program, benefit, or other offering, including payments to consumers, related tofor the collection, deletion,retention, or sale, or sharing of personal information. Price or service differences are types of financial incentives.

(m) "First party" means a consumer-facing business with which the consumer intends and expects to interact.

(n) "Frictionless manner" means a business's processing of an opt-out preference signal that complies with the requirements set forth in section 7025, subsection (f).

(o) "Information practices" means practices regarding the collection, use, disclosure, sale, sharing, and retention of personal information.

(p) "Nonbusiness" means a person or entity that does not meet the definition of a "business" as defined in Civil Code section 1798.140, subdivision (d). For example, non-profits and government entities are nonbusinesses because "business" is defined, among other things, to include only entities "organized or operated for the profit or financial benefit of its shareholders or other owners."

(q) "Notice at Collection" means the notice given by a business to a consumer at or before the point at which a business collects personal information from the consumer as required by Civil Code section 1798.100, subdivisions (a) and (b), and specified in these regulations.

(r) "Notice of Right to Limit" means the notice given by a business informing consumers of their right to limit the use or disclosure of the consumer's sensitive personal information as required by Civil Code sections 1798.121 and 1798.135 and specified in these regulations.

(s) "Notice of Right to Opt-out of Sale/Sharing" means the notice given by a business informing consumers of their right to opt-out of the sale or sharing of their personal information as required by Civil Code sections 1798.120 and 1798.135 and specified in these regulations.

(t) "Notice of Financial Incentive" means the notice given by a business explaining each financial incentive or price or service difference as required by Civil Code section 1798.125, subdivision (b), and specified in these regulations.

(u) "Opt-out preference signal" means a signal that is sent by a platform, technology, or mechanism, on behalf of the consumer, that communicates the consumer choice to opt-out of the sale and sharing of personal information and that complies with the requirements set forth in section 7025, subsection (b).

(v) "Price or service difference" means (1) any difference in the price or rate charged for any goods or services to any consumer related to the collection, retention, or sale, or sharing of personal information; or (2) any difference in the level or quality of any goods or services offered to any consumer related to the collection, retention, or sale, or sharing of personal information, including the denial of goods or services to the consumer.

(w) "Privacy policy," as referred to in Civil Code sections 1798.130, subdivision (a)(5), and 1798.135, subdivision (c)(2), means the statement that a business shall make available to consumers describing the business's online and offline information practices, and the rights of consumers regarding their own personal information.

(x) "Request to correct" means a consumer request that a business correct inaccurate personal information that it maintains about the consumer, pursuant to Civil Code section 1798.106.

(y) "Request to delete" means a consumer request that a business delete personal information about the consumer that the business has collected from the consumer, pursuant to Civil Code section 1798.105.

(z) "Request to know" means a consumer request that a business disclose personal information that it has collected about the consumer pursuant to Civil Code sections 1798.110, or 1798.115. It includes a request for any or all of the following: (1) Specific pieces of personal information that a business has collected about the consumer; (2) Categories of personal information it has collected about the consumer; (3) Categories of sources from which the personal information is collected; (4) Categories of personal information that the business sold or disclosed for a business purpose about the consumer; (5) Categories of third parties to whom the personal information was sold or disclosed for a business purpose; and (6) The business or commercial purpose for collecting or selling personal information.

(aa) "Request to limit" means a consumer request that a business limit the use and disclosure of the consumer's sensitive personal information, pursuant to Civil Code section 1798.121, subdivision (a).

(bb) "Request to opt-in to sale/sharing" means an action demonstrating that the consumer has consented to the business's sale or sharing of personal information about the consumer by a parent or guardian of a consumer less than 13 years of age, or by a consumer at least 13 years of age.

(cc) "Request to opt-out of sale/sharing" means a consumer request that a business neither sell nor share the consumer's personal information to third parties, pursuant to Civil Code section 1798.120, subdivision (a).

(dd) "Right to correct" means the consumer's right to request that a business correct inaccurate personal information that it maintains about the consumer as set forth in Civil Code section 1798.106.

(ee) "Right to delete" means the consumer's right to request that a business delete any personal information about the consumer that the business has collected from the consumer as set forth in Civil Code section 1798.105.

(ff) "Right to know" means the consumer's right to request that a business disclose personal information that it has collected, sold, or shared about the consumer as set forth in Civil Code sections 1798.110 and 1798.115.

(gg) "Right to limit" means the consumer's right to request that a business limit the use and disclosure of a consumer's sensitive personal information as set forth in Civil Code section 1798.121.

(hh) "Right to opt-out of sale/sharing" means the consumer's right to direct a business that sells or shares personal information about the consumer to third parties to stop doing so as set forth in Civil Code section 1798.120.

(ii) "Signed" means that the written attestation, declaration, or permission has either been physically signed or provided electronically in accordance with the Uniform Electronic Transactions Act, Civil Code section 1633.1 et seq.

(jj) "Third-party identity verification service" means a security process offered by an independent third party that verifies the identity of the consumer making a request to the business. Third-party identity verification services are subject to the requirements set forth in Article 5 regarding and requests to delete, requests to correct, or requests to know.

(kk) "Unstructured" as it relates to personal information means personal information that is not organized in a pre-defined manner and could not be retrieved or organized in a pre-defined manner without disproportionate effort on behalf of the business, service provider, contractor, or third party.

(ll) "Value of the consumer's data" means the value provided to the business by the consumer's data as calculated under section 7081.

(mm) "Verify" means to determine that the consumer making request to delete, request to correct, or request to know is the consumer about whom the business has collected information, or if that consumer is less than 13 years of age, the consumer's parent or legal guardian.

Note: Authority cited: Sections 1798.175 and 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145, 1798.150, 1798.155, 1798.175, 1798.185, 1798.199.40, 1798.199.45, 1798.199.50, 1798.199.55 and 1798.199.65, Civil Code

11 C.F.R. § 7002. Restrictions on the Collection and Use of Personal Information

(a) In accordance with Civil Code section 1798.100, subdivision (c), a business's collection, use, retention, and/or sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve:

(1) The purpose(s) for which the personal information was collected or processed, which shall comply with the requirements set forth in subsection (b); or

(2) Another disclosed purpose that is compatible with the context in which the personal information was collected, which shall comply with the requirements set forth in subsection (c).

(b) The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer(s) whose personal information is collected or processed. The consumer's (or consumers') reasonable expectations concerning the purpose for which their personal information will be collected or processed shall be based on the following:

(1) The relationship between the consumer(s) and the business. For example, if the consumer is intentionally interacting with the business on its website to purchase a good or service, the consumer likely expects that the purpose for collecting or processing the personal information is to provide that good or service. By contrast, for example, the consumer of a business's mobile flashlight application would not expect the business to collect the consumer's geolocation information to provide the flashlight service.

(2) The type, nature, and amount of personal information that the business seeks to collect or process. For example, if a business's mobile communication application requests access to the consumer's contact list in order to call a specific individual, the consumer who is providing their contact list likely expects that the purpose of the business's use of that contact list will be to connect the consumer with the specific contact they selected. Similarly, if a business collects the consumer's fingerprint in connection with setting up the security feature of unlocking the device using the fingerprint, the consumer likely expects that the business's use of the consumer's fingerprint is only for the purpose of unlocking their mobile device.

(3) The source of the personal information and the business's method for collecting or processing it. For example, if the consumer is providing their personal information directly to the business while using the business's product or service, the consumer likely expects that the business will use the personal information to provide that product or service. However, the consumer may not expect that the business will use that same personal information for a different product or service offered by the business or the business's subsidiary.

(4) The specificity, explicitness, prominence, and clarity of disclosures to the consumer(s) about the purpose for collecting or processing their personal information, such as in the Notice at Collection and in the marketing materials to the consumer(s) about the business's good or service. For example, the consumer who receives a pop-up notice that the business wants to collect the consumer's phone number to verify their identity when they log in likely expects that the business will use their phone number for the purpose of verifying the consumer's identity and not for marketing purposes. Similarly, the consumer may expect that a mobile application that markets itself as a service that finds gas prices near the consumer's location will collect and use the consumer's geolocation information for that specific purpose when they are using the service.

(5) The degree to which the involvement of service providers, contractors, third parties, or other entities in the collecting or processing of personal information is apparent to the consumer(s). For example, the consumer likely expects an online retailer's disclosure of the consumer's name and address to a delivery service provider in order for that service provider to deliver a purchased product, because that service provider's involvement is apparent to the consumer. By contrast, the consumer may not expect the disclosure of personal information to a service provider if the consumer is not directly interacting with the service provider or the service provider's role in the processing is not apparent to the consumer.

(c) Whether another disclosed purpose is compatible with the context in which the personal information was collected shall be based on the following:

(1) At the time of collection of the personal information, the reasonable expectations of the consumer(s) whose personal information is collected or processed concerning the purpose for which their personal information will be collected or processed, based on the factors set forth in subsection (b).

(2) The other disclosed purpose for which the business seeks to further collect or process the consumer's personal information, including whether it is a business purpose listed in Civil Code section 1798.140, subdivisions (e)(1) through (e)(8).

(3) The strength of the link between subsection (c)(1) and subsection (c)(2). For example, a strong link exists between the consumer's reasonable expectations that the personal information will be used to provide them with a requested service at the time of collection, and the use of the information to repair errors that impair the intended functionality of that requested service. This would weigh in favor of compatibility. By contrast, for example, a weak link exists between the consumer's reasonable expectations that the personal information will be collected to provide a requested cloud storage service at the time of collection, and the use of the information to research and develop an unrelated facial recognition service.

(d) For each purpose identified in compliance with subsection (a)(1) or (a)(2), the collection, use, retention, and/or sharing of a consumer's personal information to achieve that purpose shall be reasonably necessary and proportionate. The business's collection, use, retention, and/or sharing of a consumer's personal information shall also be reasonably necessary and proportionate to achieve any purpose for which the business obtains the consumer's consent in compliance with subsection (e). Whether a business's collection, use, retention, and/or sharing of a consumer's personal information is reasonably necessary and proportionate to achieve the purpose identified in compliance with subsection (a)(1) or (a)(2), or any purpose for which the business obtains consent, shall be based on the following:

(1) The minimum personal information that is necessary to achieve the purpose identified in compliance with subsection (a)(1) or (a)(2), or any purpose for which the business obtains consent. For example, to complete an online purchase and send an email confirmation of the purchase to the consumer, an online retailer may need the consumer's order information, payment and shipping information, and email address.

(2) The possible negative impacts on consumers posed by the business's collection or processing of the personal information. For example, a possible negative impact of collecting precise geolocation information is that it may reveal other sensitive personal information about the consumer, such as health information based on visits to healthcare providers.

(3) The existence of additional safeguards for the personal information to specifically address the possible negative impacts on consumers considered by the business in subsection (d)(2). For example, a business may consider encryption or automatic deletion of personal information within a specific window of time as potential safeguards.

(e) A business shall obtain the consumer's consent in accordance with section 7004 before collecting or processing personal information for any purpose that does not meet the requirements set forth in subsection (a).

(f) A business shall not collect categories of personal information other than those disclosed in its Notice at Collection in accordance with the CCPA and section 7012. If the business intends to collect additional categories of personal information or intends to use the personal information for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected, the business shall provide a new Notice at Collection. However, any additional collecting or processing of personal information shall comply with subsection (a).

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.106, 1798.121, 1798.130, 1798.135 and 1798.185, Civil Code.

11 C.F.R. § 7003. Requirements for Disclosures and Communications to Consumers

(a) Disclosures and communications to consumers shall be easy to read and understandable to consumers. For example, they shall use plain, straightforward language and avoid technical or legal jargon.

(b) Disclosures required under Article 2 shall also:

(1) Use a format that makes the disclosure readable, including on smaller screens, if applicable.

(2) Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.

(3) Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the policy in an alternative format.

(c) For websites, a conspicuous link required under the CCPA or these regulations shall appear in a similar manner as other similarly-posted links used by the business on its homepage(s). For example, the business shall use a font size and color that is at least the approximate size or color as other links next to it that are used by the business on its homepage(s).

(d) For mobile applications, a conspicuous link shall be included in the business's privacy policy, which must be accessible through the mobile application's platform page or download page. It may also be accessible through a link within the application, such as through the application's settings menu.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130 and 1798.135, Civil Code.

11 C.F.R. § 7004. Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent

(a) Except as expressly allowed by the CCPA and these regulations, businesses shall design and implement methods for submitting CCPA requests and obtaining consumer consent that incorporate the following principles:

(1) Easy to understand. The methods shall use language that is easy for consumers to read and understand. When applicable, they shall comply with the requirements for disclosures to consumers set forth in section 7003.

(2) Symmetry in choice. The path for a consumer to exercise a more privacy-protective option shall not be longer or more difficult or time-consuming than the path to exercise a less privacy-protective option because that would impair or interfere with the consumer's ability to make a choice. Illustrative examples follow.

(A) It is not symmetrical when a business's process for submitting a request to opt-out of sale/sharing requires more steps than that business's process for a consumer to opt-in to the sale of personal information after having previously opted out. The number of steps for submitting a request to opt-out of sale/sharing is measured from when the consumer clicks on the "Do Not Sell or Share My Personal Information" link to completion of the request. The number of steps for submitting a request to opt-in to the sale of personal information is measured from the first indication by the consumer to the business of their interest to opt-in to completion of the request.

(B) A choice to opt-in to the sale of personal information that provides only the two options, "Yes" and "Ask me later," is not equal or symmetrical because there is no option to decline the opt-in. "Ask me later" implies that the consumer has not declined but delayed the decision and that the business will continue to ask the consumer to opt-in. Framing

the consumer's options in this manner impairs the consumer's ability to make a choice. An equal or symmetrical choice could be between "Yes" and "No."

(C) A website banner that provides only the two options, "Accept All" and "More Information," or, "Accept All" and "Preferences," when seeking the consumer's consent to use their personal information is not equal or symmetrical because the method allows the consumer to "Accept All" in one step, but requires the consumer to take additional steps to exercise their rights over their personal information. Framing the consumer's options in this manner impairs the consumer's ability to make a choice. An equal or symmetrical choice could be between "Accept All" and "Decline All."

(3) Avoid language or interactive elements that are confusing to the consumer. The methods should not use double negatives. Toggles or buttons must clearly indicate the consumer's choice. Illustrative examples follow.

(A) Giving the choice of "Yes" or "No" next to the statement "Do Not Sell or Share My Personal Information" is a double negative and a confusing choice for a consumer.

(B) Toggles or buttons that state "on" or "off" may be confusing to a consumer and may require further clarifying language.

(C) Unintuitive placement of buttons to confirm a consumer's choice may be confusing to the consumer. For example, it is confusing to the consumer when a business at first consistently offers choices in the order of "Yes," then "No," but then offers choices in the opposite order—"No," then "Yes"—when asking the consumer something that would contravene the consumer's expectation.

(4) Avoid choice architecture that impairs or interferes with the consumer's ability to make a choice. Businesses should also not design their methods in a manner that would impair the consumer's ability to exercise their choice because consent must be freely given, specific, informed, and unambiguous. Illustrative examples follow.

(A) Requiring the consumer to click through disruptive screens before they are able to submit a request to opt-out of sale/sharing is a choice architecture that impairs or interferes with the consumer's ability to exercise their choice.

(B) Bundling choices so that the consumer is only offered the option to consent to using personal information for purposes that meet the requirements set forth in section 7002, subsection (a), together with purposes that are incompatible with the context in which the personal information was collected is a choice architecture that impairs or interferes with the consumer's ability to make a choice. For example, a business that provides a location-based service, such as a mobile application that finds gas prices near the consumer's location, shall not require the consumer to consent to incompatible uses (e.g., sale of the consumer's geolocation to data brokers) together with a reasonably necessary and proportionate use of geolocation information for providing the location-based services, which does not require consent. This type of choice architecture does not allow consent to be freely given, specific, informed, or unambiguous because it requires the consumer to consent to incompatible uses in order to obtain the expected service. The business should provide the consumer a separate option to consent to the business's use of personal information that does not meet the requirements set forth in section 7002, subsection (a).

(5) Easy to execute. The business shall not add unnecessary burden or friction to the process by which the consumer submits a CCPA request. Methods should be tested to ensure that they are functional and do not undermine the consumer's choice to submit the request. Illustrative examples follow.

(A) Upon clicking the "Do Not Sell or Share My Personal Information" link, the business shall not require the consumer to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out of sale/sharing.

(B) A business that knows of, but does not remedy, circular or broken links, or nonfunctional email addresses, such as inboxes that are not monitored or have aggressive filters that screen emails from the public, may be in violation of this regulation.

(C) Businesses that require the consumer to unnecessarily wait on a webpage as the business processes the request may be in violation of this regulation.

(b) A method that does not comply with subsection (a) may be considered a dark pattern. Any agreement obtained through the use of dark patterns shall not constitute consumer consent. For example, a business that uses dark patterns to obtain consent from a consumer to sell their personal information shall be in the position of never having obtained the consumer's consent to do so.

(c) A user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decision making, or choice. A business's intent in designing the interface is not determinative in whether the user interface is a dark pattern, but a factor to be considered. If a business did not intend to design the user interface to subvert or impair user choice, but the business knows of and does not remedy a user interface that has that effect, the user interface may still be a dark pattern. Similarly, a business's deliberate ignorance of the effect of its user interface may also weigh in favor of establishing a dark pattern.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.

Article 2. REQUIRED DISCLOSURES TO CONSUMERS

11 C.F.R. § 7010. Overview of Required Disclosures

(a) Every business that must comply with the CCPA and these regulations shall provide a privacy policy in accordance with the CCPA and section 7011.

(b) A business that controls the collection of a consumer's personal information from a consumer shall provide a Notice at Collection in accordance with the CCPA and section 7012.

(c) Except as set forth in section 7025, subsection (g), A business that sells or shares personal information shall provide a Notice of Right to Opt-out of Sale/Sharing or the Alternative Opt-out Link in accordance with the CCPA and sections 7013 and 7015.

(d) A business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in section 7027, subsection (m), shall provide a Notice of Right to Limit or the Alternative Opt-out Link in accordance with the CCPA and sections 7014 and 7015.

(e) A business that offers a financial incentive or price or service difference shall provide a Notice of Financial Incentive in accordance with the CCPA and section 7016.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130 and 1798.135, Civil Code.

11 C.F.R. § 7011. Privacy Policy

(a) The purpose of the privacy policy is to provide consumers with a comprehensive description of a business's online and offline information practices regarding the collection, use, disclosure, and sale of personal information. It shall also inform consumers about and of the rights of consumers they have regarding their personal information and provide any information necessary for them to exercise those rights.

(b) The privacy policy shall comply with section 7003, subsections (a) and (b).

(c) The privacy policy shall be available in a format that allows a consumer to print it out as a document.

(d) The privacy policy shall be posted online and accessible through a conspicuous link that complies with section 7003, subsections (c) and (d), using the word "privacy" on the business's website homepage(s) or on the download or landing page of a mobile application. If the business has a California-specific description of consumers' privacy rights on its website, then the privacy policy shall be included in that description. A business that does not operate a website shall make the privacy policy conspicuously available to consumers. A mobile application may include a link to the privacy policy in the application's settings menu.

(e) The privacy policy shall include the following information:

(1) A comprehensive description of the business's online and offline information practices, which includes the following:

(A) Identification of the categories of personal information the business has collected about consumers in the preceding 12 months. The categories shall be described using the specific terms set forth in Civil Code section 1798.140, subdivisions (v)(1)(A) to (K) and (ae)(1) to (2). To the extent that the business has discretion in its description, the business shall describe the category in a manner that provides consumers a meaningful understanding of the information being collected.

(B) Identification of the categories of sources from which the personal information is collected.

(C) Identification of the specific business or commercial purpose for collecting personal information from consumers. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is collected.

(D) Identification of the categories of personal information, if any, that the business has sold or shared to third parties in the preceding 12 months. If the business has not sold or shared consumers' personal information in the preceding 12 months, the business shall disclose that fact.

(E) For each category of personal information identified in subsection (e)(1)(D), the categories of third parties to whom the information was sold or shared.

(F) Identification of the specific business or commercial purpose for selling or sharing consumers' personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is sold or shared.

(G) A statement regarding whether the business has actual knowledge that it sells or shares the personal information of consumers under 16 years of age.

(H) Identification of the categories of personal information, if any, that the business has disclosed for a business purpose to third parties in the preceding 12 months. If the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(I) For each category of personal information identified in subsection (e)(1)(H), the categories of third parties to whom the information was disclosed.

(J) Identification of the specific business or commercial purpose for disclosing the consumer's personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is disclosed.

(K) A statement regarding whether the business uses or discloses sensitive personal information for purposes other than those specified in section 7027, subsection (m).

(2) An explanation of the rights that the CCPA confers on consumers regarding their personal information, which includes all of the following:

(A) The right to know what personal information the business has collected about the consumer, including the categories of personal information, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting, selling, or sharing personal information, the categories of third parties to whom the business discloses personal information, and the specific pieces of personal information the business has collected about the consumer.

(B) The right to delete personal information that the business has collected from the consumer, subject to certain exceptions.

(C) The right to correct inaccurate personal information that a business maintains about a consumer.

(D) If the business sells or shares personal information, the right to opt-out of the sale or sharing of their personal information by the business.

(E) If the business uses or discloses sensitive personal information for reasons other than those set forth in section 7027, subsection (m), the right to limit the use or disclosure of sensitive personal information by the business.

(F) The right not to receive discriminatory treatment by the business for the exercise of privacy rights conferred by the CCPA, including an employee's, applicant's, or independent contractor's right not to be retaliated against for the exercise of their CCPA rights.

(3) An explanation of how consumers can exercise their CCPA rights and what consumers can expect from that process, which includes all of the following:

(A) An explanation of the methods by which the consumer can exercise their CCPA rights.

(B) Instructions for submitting a request under the CCPA, including any links to an online request form or portal for making such a request, if offered by the business.

(C) If the business sells or shares personal information, and is required to provide aNotice of Right to Opt-out of Sale/Sharing, the contents of the Notice of Right to Opt-out of Sale/Sharing or a link to that notice in accordance with section 7013, subsection (f).

(D) If the business uses or discloses sensitive personal information for purposes other than those specified in section 7027, subsection (m), and is required to provide a Notice of Right to Limit, the contents of the Notice of Right to Limit or a link to that notice in accordance with section 7014, subsection (f).

(E) A general description of the process the business uses to verify a consumer request to know, request to delete, and request to correct, when applicable, including any information the consumer must provide.

(F) Explanation of how an opt-out preference signal will be processed for the consumer (i.e., whether the signal applies to the device, browser, consumer account, and/or offline sales, and in what circumstances) and how the consumer can use an opt-out preference signal.

(G) If the business processes opt-out preference signals in a frictionless manner, information on how consumers can implement opt-out preference signals for the business to process in a frictionless manner.

(H) Instructions on how an authorized agent can make a request under the CCPA on the consumer's behalf.

(I) If the business has actual knowledge that it sells the personal information of consumers under 16 years of age, a description of the processes required by sections 7070 and 7071.

(J) A contact for questions or concerns about the business's privacy policies and information practices using a method reflecting the manner in which the business primarily interacts with the consumer.

(4) Date the privacy policy was last updated.

(5) If subject to the data reporting requirements set forth in section 7102, the information required under section 7102, or a link to that information.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, and 1798.130 and 1798.135, Civil Code.

11 C.F.R. § 7012. Notice at Collection of Personal Information

(a) The purpose of the Notice at Collection is to provide consumers with timely notice, at or before the point of collection, about the categories of personal information to be collected from them, the purposes for which the personal information is collected or used, and whether that information is sold or shared, so that consumers have a tool to exercise meaningful control over the business's use of their personal information. For example, upon receiving the Notice at Collection, the consumer can use the information in the notice as a tool to choose whether to engage with the business, or to direct the business not to sell or share their personal information and to limit the use and disclosure of their sensitive personal information.

(b) The Notice at Collection shall comply with section 7003, subsections (a) and (b).

(c) The Notice at Collection shall be made readily available where consumers will encounter it at or before the point of collection of any personal information. Illustrative examples follow.:

(1) When a business collects consumers' personal information online, it may post a conspicuous link to the notice on the introductory page of the business's website and on all webpages where personal information is collected.

(2) When a business collects consumers' personal information through a webform, it may post a conspicuous link to the notice in close proximity to the fields in which the consumer inputs their personal information, or in close proximity to the button by which the consumer submits their personal information to the business.

(3) When a business collects personal information through a mobile application, it may provide a link to the notice on the mobile application's download page and within the application, such as through the application's settings menu.

(4) When a business collects consumers' personal information offline, it may include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to where the notice can be found online.

(5) When a business collects personal information over the telephone or in person, it may provide the notice orally.

(d) If a business does not give the Notice at Collection to the consumer at or before the point of collection of their personal information, the business shall not collect personal information from the consumer.

(e) A business shall include the following in its Notice at Collection:

(1) A list of the categories of personal information about consumers, including categories of sensitive personal information, to be collected. Each category of personal information shall be written in a manner that provides consumers a meaningful understanding of the information being collected.

(2) The purpose(s) for which the categories of personal information, including categories of sensitive personal information, are collected and used.

(3) Whether each category of personal information identified in subsection (e)(1) is sold or shared.

(4) The length of time the business intends to retain each category of personal information identified in subsection (e)(1), or if that is not possible, the criteria used to determine the period of time it will be retained.

(5) If the business sells or shares personal information, the link to the Notice of Right to Opt-out of Sale/Sharing or in the case of offline notices, where the webpage can be found online.

(6) A link to the business's privacy policy, or in the case of offline notices, where the privacy policy can be found online.

(f) If a business collects personal information from a consumer online, the Notice at Collection may be given to the consumer by providing a link that takes the consumer directly to the specific section of the business's privacy policy that contains the information required in subsection (e)(1) through (6). Directing the consumer to the beginning of the privacy policy, or to another section of the privacy policy that does not contain the required information, so that the consumer is required to scroll through other information in order to determine the categories of personal information to be collected and/or whether the business sells or shares the personal information collected, does not satisfy this standard.

(g) Third Parties that Control the Collection of Personal Information. This subsection shall not affect the first party's obligations under the CCPA to comply with a consumer's request to opt-out of sale/sharing.

(1) For purposes of giving Notice at Collection, more than one business may control the collection of a consumer's personal information, and thus, have an obligation to provide a Notice at Collection in accordance with the CCPA and these regulations. For example, a first party may allow another business, acting as a third party, to control the collection of personal information from consumers browsing the first party's website. Both the first party that allows the third parties to collect personal information via its website, as well as the third party controlling the collection of personal information, shall provide a Notice at Collection. The first party and third parties may provide a single Notice at Collection that includes the required information about their collective information practices.

(2) A business that, acting as a third party, controls the collection of personal information on another business's physical premises, such as in a retail store or in a vehicle, shall provide a Notice at Collection in a conspicuous manner at the physical location(s) where it is collecting the personal information.

(3) Illustrative examples follow.

(A) Business F allows Business G, a third party ad network, to collect consumers' personal information through Business F's website. Business F may post a conspicuous link to its Notice at Collection on its homepage(s). Business G shall provide a Notice at Collection on its homepage(s) or include the required information about its information practices in Business F's Notice at Collection.

(B) Business H, a coffee shop, allows Business I, a business providing Wi-Fi services, to collect personal information from consumers using Business I's services on Business H's premises. Business H may post conspicuous signage at the entrance of the store or at the point-of-sale directing consumers to where the Notice at Collection for Business H can be found online. In addition, Business I shall post its own Notice at Collection on the first webpage or other interface consumers see before connecting to the Wi-Fi services offered.

(C) Business J, a car rental business, allows Business K to collect personal information from consumers within the vehicles Business J rents to consumers. Business J may give its Notice at Collection to the consumer at the point of sale (i.e., at the rental counter) either in writing or orally. Business K may provide its own Notice at Collection within the vehicle, such as through signage on the vehicle's dashboard directing consumers to where the notice can be found online.

(h) A business that neither collects nor controls the collection of personal information directly from the consumer does not need to provide a Notice at Collection to the consumer if it neither sells nor shares the consumer's personal information.

(i) A data broker registered with the Attorney General pursuant to Civil Code section 1798.99.80 et seq. that collects personal information from a source other than directly from the consumer does not need to provide a Notice at Collection to the consumer if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out of sale/sharing.

Note: Authority: Section 1798.185, Civil Code. Reference: Sections 1798.99.82, 1798.100, 1798.115, 1798.120, 1798.121, 1798.145 and 1798.185, Civil Code.

11 C.F.R. § 7013. Notice of Right to Opt-out of Sale/Sharing and the "Do Not Sell or Share My Personal Information" Link

(a) The purpose of the Notice of Right to Opt-out of Sale/Sharing is to inform consumers of their right to direct a business that sells or shares their personal information to stop selling or sharing their personal information and to provide them with the opportunity to exercise that right. The purpose of the "Do Not Sell or Share My Personal Information" link is to immediately effectuate the consumer's right to opt-out of sale/sharing, or in the alternative, direct the consumer to the Notice of Right to Opt-out of Sale/Sharing. Accordingly, clicking the business's "Do Not Sell or Share My Personal Information" link will either have the immediate effect of opting the consumer out of the sale or sharing of personal information or lead the consumer to a webpage where the consumer can learn about and make that choice.

(b) The Notice of Right to Opt-out of Sale/Sharing shall comply with section 7003, subsections (a) and (b).

(c) The "Do Not Sell or Share My Personal Information" link shall be a conspicuous link that complies with section 7003, subsections (c) and (d) and is located at either the header or footer of the business's internet homepage(s).

(d) In lieu of posting the "Do Not Sell or Share My Personal Information" link, a business may provide the Alternative Opt-out Link in accordance with section 7015 or process opt-out preference signals in a frictionless manner in accordance with section 7025, subsections (f) and (g). The business must still post a Notice of Right to Opt-out of Sale/Sharing in accordance with these regulations.

(e) A business that sells or shares the personal information of consumers shall provide the Notice of Right to Opt-out of Sale/Sharing to consumers as follows:

(1) A business shall post the Notice of Right to Opt-out of Sale/Sharing on the internet webpage to which the consumer is directed after clicking on the "Do Not Sell or Share My Personal Information" link. The notice shall include the information specified in subsection (f) or be a link that takes the consumer directly to the specific section of the business's privacy policy that contains the same information. If clicking on the "Do Not Sell or Share My Personal

Information" link immediately effectuates the consumer's right to opt-out of sale/sharing or if the business processes opt-out preference signals in a frictionless manner and chooses not to post a link, the business shall provide the notice within its privacy policy.

(2) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their right to opt-out of sale/sharing. That method shall comply with the requirements set forth in section 7003.

(3) A business shall also provide the notice to opt-out of sale/sharing in the same manner in which it collects the personal information that it sells or shares. Illustrative examples follow.

(A) A business that sells or shares personal information that it collects in the course of interacting with consumers offline, such as in a brick-and-mortar store, shall provide notice through an offline method, e.g., on the paper forms that collect the personal information or by posting signage in the area where the personal information is collected directing consumers to where the notice can be found online.

(B) A business that sells or shares personal information that it collects over the phone may shall provide notice inform consumers of their right to opt-out orally during the call when the information is collected.

(f) A business shall include the following in its Notice of Right to Opt-out of Sale/Sharing: (1) A description of the consumer's right to opt-out of the sale or sharing of their personal information by the business; and (2) Instructions on how the consumer can submit a request to opt-out of sale/sharing. If notice is provided online, the notice shall include the interactive form by which the consumer can submit their request to opt-out of sale/sharing online, as required by section 7026, subsection (a)(1). If the business does not operate a website, the notice shall explain the offline method by which the consumer can submit their request to opt-out of sale/sharing.

(g) A business does not need to provide a Notice of Right to Opt-out of Sale/Sharing or the "Do Not Sell or Share My Personal Information" link if: (1) It does not sell or share personal information; and (2) It states in its privacy policy that it does not sell or share personal information. (h) (e) A business shall not sell or share the personal information it collected during the time the business did not have a Notice of Right to Opt-out of Sale/Sharing posted unless it obtains the consent of the consumer.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

11 C.F.R. § 7014. Notice of Right to Limit and the "Limit the Use of My Sensitive Personal Information" Link.

(a) The purpose of the Notice of Right to Limit is to inform consumers of their right to limit a business's use and disclosure of their sensitive personal information and to provide them with the opportunity to exercise that right. The purpose of the "Limit the Use of My Sensitive Personal Information" link is to immediately effectuate the consumer's right to limit, or in the alternative, direct the consumer to the Notice of Right to Limit. Accordingly, clicking the business's "Limit the Use of My Sensitive Personal Information" link will either have the immediate effect of limiting the use and disclosure of the consumer's sensitive personal information or lead the consumer to a webpage where the consumer can learn about and make that choice.

(b) The Notice of Right to Limit shall comply with section 7003, subsections (a) and (b).

(c) The "Limit the Use of My Sensitive Personal Information" link shall be a conspicuous link that complies with section 7003, subsections (c) and (d), and is located at either the header or footer of the business's internet homepage(s).

(d) In lieu of posting the "Limit the Use of My Sensitive Personal Information" link, a business may provide the Alternative Opt-out Link in accordance with section 7015. The business shall still post a Notice of Right to Limit in accordance with these regulations.

(e) A business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in section 7027, subsection (m), shall provide the Notice of Right to Limit to consumers as follows:

(1) A business shall post the Notice of Right to Limit on the internet webpage to which the consumer is directed after clicking on the "Limit the Use of My Sensitive Personal Information" link. The notice shall include the information specified in subsection (f) or be a link that takes the consumer directly to the specific section of the business's privacy policy that contains the same information. If clicking on the "Limit the Use of My Sensitive Personal Information" link immediately effectuates the consumer's right to limit, the business shall provide the notice within its privacy policy.

(2) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their right to limit. That method shall comply with the requirements set forth in section 7003.

(f) A business shall include the following in its Notice of Right to Limit:

(1) A description of the consumer's right to limit; and

(2) Instructions on how the consumer can submit a request to limit. If notice is provided online, the notice shall include the interactive form by which the consumer can submit their request to limit online, as required by section 7027, subsection (b)(1). If the business does not operate a website, the notice shall explain the offline method by which the consumer can submit their request to limit.

(g) A business does not need to provide a Notice of Right to Limit or the "Limit the Use of My Sensitive Personal Information" link if:

(1) It only uses and discloses sensitive personal information that it collected about the consumer for the purposes specified in section 7027, subsection (m), and states so in its privacy policy; or

(2) It only collects or processes sensitive personal information without the purpose of inferring characteristics about a consumer, and states so in its privacy policy. (h) A business shall not use or disclose sensitive personal information it collected during the time the business did not have a Notice of Right to Limit posted for purposes other than those specified in section 7027, subsection (m), unless it obtains the consent of the consumer.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.121, 1798.135 and 1798.185, Civil Code.

11 C.F.R. § 7015. Alternative Opt-out Link

(a) The purpose of the Alternative Opt-out Link is to provide businesses the option of providing consumers with a single, clearly-labeled link that allows consumers to easily exercise both their right to opt-out of sale/sharing and right to limit, instead of posting the two separate "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links. The Alternative Opt-out Link shall direct the consumer to a webpage that informs them of both their right to opt-out of sale/sharing and right to limit and provides them with the opportunity to exercise both rights.

(b) A business that chooses to use an Alternative Opt-out Link shall title the link, "Your Privacy Choices," or, "Your California Privacy Choices," and shall include the following opt-out icon adjacent to the title. The link shall be a conspicuous link that complies with section 7003, subsections (c) and (d), and is located at either the header or footer of the business's internet homepage(s). The icon shall be approximately the same size as other icons used by the business in the header or footer of its webpage.

(c) The Alternative Opt-out Link shall direct the consumer to a webpage that includes the following information:

(1) A description of the consumer's right to opt-out of sale/sharing and right to limit, which shall comply with section 7003, subsections (a) and (b); and

(2) The interactive form or mechanism by which the consumer can submit their request to opt-out of sale/sharing and their right to limit online. The method shall be easy for consumers to execute, shall require minimal steps, and shall comply with section 7004.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.121, 1798.135 and 1798.185, Civil Code.

11 C.F.R. § 7016. Notice of Financial Incentive

(a) The purpose of the Notice of Financial Incentive is to explain to the consumer the material terms of a financial incentive or price or service difference the business is offering so that the consumer may make an informed decision about whether to participate. A business that does not offer a financial incentive or price or service difference is not required to provide a Notice of Financial Incentive.

(b) The Notice of Financial Incentive shall comply with section 7003, subsections (a) and (b).

(c) The Notice of Financial Incentive shall be readily available where consumers will encounter it before opting-in to the financial incentive or price or service difference. If the business offers the financial incentive or price or service difference online, the notice may be given by providing a link that takes the consumer directly to the specific section of a business's privacy policy that contains the information required in subsection (d).

(d) A business shall include the following in its Notice of Financial Incentive:

(1) A succinct summary of the financial incentive or price or service difference offered;

(2) A description of the material terms of the financial incentive or price or service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference and the value of the consumer's data;

(3) How the consumer can opt-in to the financial incentive or price or service difference;

(4) A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and

(5) An explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, including:

(A) A good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and

(B) A description of the method(s) the business used to calculate the value of the consumer's data.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125 and 1798.130, Civil Code.

Article 3. BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS

11 C.F.R. § 7020. Methods for Submitting Requests to Delete, Requests to Correct, and Requests to Know

(a) A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests to delete, requests to correct, and requests to know.

(b) A business that does not fit the description in subsection (a) shall provide two or more designated methods for submitting requests to delete, requests to correct, and requests to know. One of those methods must be a toll-free telephone number. If the business maintains an internet website, one of the methods for submitting these requests shall be through its website, such as through a webform. Other Acceptable methods for submitting these requests to delete, requests to correct, and requests to know may include, but are not limited to, a designated email address, a form submitted in person, and a form submitted through the mail.

(c) A business shall consider the methods by which it primarily interacts with consumers when determining which methods to provide for submitting requests to delete, requests to correct, and requests to know. If the business interacts with consumers in person, the business shall consider providing an in-person method such as a printed form the consumer can directly submit or send by mail, a tablet or computer portal that allows the consumer to complete and submit an online form, or a telephone with which the consumer can call the business's toll-free number.

(d) A business may use a two-step process for online requests to delete where the consumer must first, submit the request to delete and then second, separately confirm that they want their personal information deleted provided that the business otherwise complies with section 7004.

(e) If a consumer submits a request in a manner that is not one of the designated methods of submission, or is deficient in some manner unrelated to the verification process, the business shall either:

(1) Treat the request as if it had been submitted in accordance with the business's designated manner, or

(2) Provide the consumer with information on how to submit the request or remedy any deficiencies with the request, if applicable.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.130, 1798.140 and 1798.185, Civil Code.

11 C.F.R. § 7021. Timelines for Responding to Requests to Delete, Requests to Correct, and Requests to Know

(a) No later than 10 business days after receiving a request to delete, request to correct, or request to know, a business shall confirm receipt of the request and provide information about how the business will process the request. The information provided shall describe in general the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request. The confirmation may be given in the same manner in which the request was received. For example, if the request is made over the phone, the confirmation may be given orally during the phone call.

(b) Businesses shall respond to a request to delete, request to correct, and request to know no later than 45 calendar days after receipt of the request. The 45- day period will begin on the day that the business receives the request, regardless of time required to verify the request. If the business cannot verify the consumer within the 45-day time period, the business may deny the request. If necessary, businesses may take up to an additional 45 calendar days to respond to the consumer's request, for a maximum total of 90 calendar days from the day the request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.130, 1798.140 and 1798.185, Civil Code.

11 C.F.R. § 7022. Requests to Delete

(a) For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 5, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified.

(b) A business shall comply with a consumer's request to delete their personal information by:

(1) Permanently and completely erasing the personal information from its existing systems except archived or back-up systems, deidentifying the personal information, or aggregating the consumer information;

(2) Notifying the business's service providers or contractors to delete from their records the consumer's personal information that they Collected pursuant to their written contract with the business, or if enabled to do so by the service provider or contractor, the business shall delete the personal information that the service provider or contractor Collected pursuant to their written contract with the business; and

(3) Notifying all third parties to whom the business has sold or shared the personal information to delete the consumer's personal information unless this proves impossible or involves disproportionate effort. If a business claims that notifying some or all third parties would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot notify all third parties. The business shall not simply state that notifying all third parties is impossible or would require disproportionate effort.

(c) A service provider or contractor shall, with respect to personal information that they Collected pursuant to their written contract with the business and upon notification by the business, cooperate with the business in responding to a request to delete by:

(1) Permanently and completely erasing the personal information from its existing systems except archived or back-up systems, deidentifying the personal information, or aggregating the consumer information, or enabling the business to do so;

(2) To the extent that an exception applies to the deletion of personal information, deleting or enabling the business to delete the consumer's personal information that is not subject to the exception and refraining from using the consumer's personal information retained for any purpose other than the purpose provided for by that exception;

(3) Notifying any of its own service providers or contractors to delete from their records in the same manner the consumer's personal information that they Collected pursuant to their written contract with the service provider or contractor; and

(4) Notifying any other service providers, contractors, or third parties that may have accessed personal information from or through the service provider or contractor, unless the information was accessed at the direction of the business, to delete the consumer's personal information unless this proves impossible or involves disproportionate effort.

(d) If a business, service provider, or contractor stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or is next accessed or used for a sale, disclosure, or commercial purpose.

(e) In responding to a request to delete, a business shall inform the consumer whether or not it has complied with the consumer's request. The business shall also inform the consumer that it will maintain a record of the request as required by section 7101, subsection (a). A business, service provider, contractor, or third party may retain a record of the request for the purpose of ensuring that the consumer's personal information remains deleted from its records.

(f) In cases where a business denies a consumer's request to delete in whole or in part, the business shall do all of the following:

(1) Provide to the consumer a detailed explanation of the basis for the denial, including any conflict with federal or state law, or exception to the CCPA, or factual basis for contending that compliance would be impossible or involve disproportionate effort, unless prohibited from doing so by law;

(2) Delete the consumer's personal information that is not subject to the exception; and

(3) Not use the consumer's personal information retained for any other purpose than provided for by that exception; and

(4) Instruct its service providers and contractors to delete the consumer's personal information that is not subject to the exception and to not use the consumer's personal information retained for any purpose other than the purpose provided for by that exception.

(g) If a business that denies a consumer's request to delete sells or shares personal information and the consumer has not already made a request to opt-out of sale/sharing, the business shall ask the consumer if they would like to opt-out of the sale or sharing of their personal information and shall include either the contents of, or a link to, the Notice of Right to Opt-out of sSale/sSharing in accordance with section 7013.

(h) In responding to a request to delete, a business may present the consumer with the choice to delete select portions of their personal information as long as a single option to delete all personal information is also offered. A business that provides consumers the ability to delete select categories of personal information (e.g., purchase history, browsing history, voice recordings) in other contexts, however, must inform consumers of their ability to do so and direct them to how they can do so. For example, a business may provide the consumer with a link to a support page or other resource that explains consumers' data deletion options.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code.

11 C.F.R. § 7023. Requests to Correct

(a) For requests to correct, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 5, the business may deny the request to correct. The business shall inform the requestor that their identity cannot be verified.

(b) In determining the accuracy of the personal information that is the subject of a consumer's request to correct, the business shall consider the totality of the circumstances relating to the contested personal information. A business may deny a consumer's request to correct if it determines that the contested personal information is more likely than not accurate based on the totality of the circumstances.

(1) Considering the totality of the circumstances includes, but is not limited to, considering:

(A) The nature of the personal information (e.g., whether it is objective, subjective, unstructured, sensitive, etc.).

(B) How the business obtained the contested information.

(C) Documentation relating to the accuracy of the information whether provided by the consumer, the business, or another source. Requirements regarding documentation are set forth in subsection (d).

(2) If the business is not the source of the personal information and has no documentation in support of the accuracy of the information, the consumer's assertion of inaccuracy may be sufficient to establish that the personal information is inaccurate.

(c) A business that complies with a consumer's request to correct shall correct the personal information at issue on its existing. The business shall also instruct all service providers and contractors that maintain the personal information at issue pursuant to their written contract with the business to make the necessary corrections in their respective systems. Service providers and contractors shall comply with the business's instructions to correct the personal information or enable the business to make the corrections. If a business, service provider, or contractor stores any personal information that is the subject of the request to correct on archived or backup systems, it may delay compliance with the consumer's request to correct, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or is next accessed or used.

(d) Documentation.

(1) A business shall accept, review, and consider any documentation that the consumer provides in connection with their right to correct whether provided voluntarily or as required by the business. Consumers should make a good-faith effort to provide businesses with all necessary information available at the time of the request.

(2) A business may require the consumer to provide documentation if necessary to rebut its own documentation that the personal information is accurate. In determining the necessity of the documentation requested, the business shall consider the following:

(A) The nature of the personal information at issue (e.g., whether it is objective, subjective, unstructured, sensitive, etc.).

(B) The nature of the documentation upon which the business considers the personal information to be accurate (e.g., whether the documentation is from a trusted source, whether the documentation is verifiable, etc.)

(C) The purpose for which the business collects, maintains, or uses the personal information. For example, if the personal information is essential to the functioning of the business, the business may require more documentation.

(D) The impact on the consumer. For example, if the personal information has a negative impact on the consumer, the business may require less documentation.

(3) Any documentation provided by the consumer in connection with their request to correct shall only be used and/or maintained by the business for the purpose of correcting the consumer's personal information and to comply with the record-keeping obligations under section 7101.

(4) The business shall implement and maintain reasonable security procedures and practices in maintaining any documentation relating to the consumer's request to correct.

(e) A business may delete the contested personal information as an alternative to correcting the information if the deletion of the personal information does not negatively impact the consumer, or the consumer consents to the deletion. For example, if deleting instead of correcting inaccurate personal information would make it harder for the consumer to obtain a job, housing, credit, education, or other type of opportunity, the business shall process the request to correct or obtain the consumer's consent to delete the information.

(f) In responding to a request to correct, a business shall inform the consumer whether or not it has complied with the consumer's request. If the business denies a consumer's request to correct in whole or in part, the business shall do the following:

(1) Explain the basis for the denial, including any conflict with federal or state law, exception to the CCPA, inadequacy in the required documentation, or contention that compliance proves impossible or involves disproportionate effort.

(2) If a business claims that complying with the consumer's request to correct would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot comply with the request. The business shall not simply state that it is impossible or would require disproportionate effort.

(3) If a business denies a consumer's request to correct personal information collected and analyzed concerning a consumer's health, the business shall also inform the consumer that they may provide a written statement to the business to be made part of the consumer's record per Civil Code section 1798.185, subdivision (a)(8)(D). The business shall explain to the consumer that the written statement is limited to 250 words per alleged inaccurate piece of personal information and shall include that the consumer must request that the statement be made part of the consumer's record. Upon receipt of such a statement, the business shall include it with the consumer's record.

(4) If the personal information at issue can be deleted pursuant to a request to delete, inform the consumer that they can make a request to delete the personal information and provide instructions on how the consumer can make a request to delete.

(g) A business may deny a consumer's request to correct if the business has denied the consumer's request to correct the same alleged inaccuracy within the past six months receiving the request. However, the business must treat the request to correct as new if the consumer provides new or additional documentation to prove that the information at issue is inaccurate.

(h) A business may deny a request to correct if it has a good-faith, reasonable, and documented belief that a request to correct is fraudulent or abusive. The business shall inform the requestor that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent or abusive.

(i) Where the business is not the source of the information that the consumer contends is inaccurate, in addition to processing the consumer's request, the business may provide the consumer with the name of the source from which the business received the alleged inaccurate information.

(j) Upon request, a business shall disclose specific pieces of personal information that the business maintains and has collected about the consumer to allow the consumer to confirm that the business has corrected the inaccurate information that was the subject of the consumer's request to correct. This disclosure shall not be considered a response to a request to know that is counted towards the limitation of two requests within a 12-month period as set forth in Civil Code section 1798.130, subdivision (b). With regard to a correction to a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics, a business shall not disclose this information, but may provide a way to confirm that the personal information it maintains is the same as what the consumer has provided.

(k) Whether a business, service provider, or contractor has implemented measures to ensure that personal information that is the subject of a request to correct remains corrected factors into whether that business, service provider, or contractor has complied with a consumer's request to correct in accordance with the CCPA and these regulations.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.106, 1798.130 1798.185, and 1798.81.5, Civil Code.

11 C.F.R. § 7024. Requests to Know

(a) For requests that seek the disclosure of specific pieces of information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 5, the business shall not disclose any specific pieces of personal information to the requestor and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall also evaluate the consumer's request as if it is seeking the disclosure of categories of personal information about the consumer pursuant to subsection (b).

(b) For requests that seek the disclosure of categories of personal information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 5, the business may deny the request to disclose the categories and other information requested and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall provide or direct the consumer to its information practices set forth in its privacy policy.

(c) In responding to a request to know, a business is not required to search for personal information if all of the following conditions are met:

(1) The business does not maintain the personal information in a searchable or reasonably accessible format;.

(2) The business maintains the personal information solely for legal or compliance purposes;.

(3) The business does not sell the personal information and does not use it for any commercial purpose;

(4) The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.

(d) A business shall not disclose in response to a request to know a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics. The business shall, however, inform the consumer with sufficient particularity that it has collected the type of information. For example, a business shall respond that it collects "unique biometric data including a fingerprint scan" without disclosing the actual fingerprint scan data.

(e) If a business denies a consumer's verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business shall inform the requestor and explain the basis for the denial, unless prohibited from doing so by law. If the request is denied only in part, the business shall disclose the other information sought by the consumer.

(f) A business shall use reasonable security measures when transmitting personal information to the consumer.

(g) If a business maintains a password-protected account with the consumer, it may comply with a request to know by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal fully discloses the personal information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 5.

(h) In response to a request to know, a business shall provide all the personal information it has collected and maintains about the consumer during the 12-month period preceding the business's receipt of the consumer's request. A consumer may request that the business provide personal information that the business collected beyond the 12-month period, as long as it was collected on or after January 1, 2022, and the business shall be required to provide that information unless doing so proves impossible or would involve disproportionate effort. That information shall include any personal information that the business's service providers or contractors collected pursuant to their written contract with the business. If a business claims that providing personal information beyond the 12-month period preceding the business's receipt of the consumer's request would be impossible or would involve disproportionate effort, the business shall not be required to provide it as long as the business provides the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot provide personal information beyond the 12-month period. The business shall not simply state that it is impossible or would require disproportionate effort.

(i) A service provider or contractor shall provide assistance to the business in responding to a verifiable consumer request to know, including by providing the business the consumer's personal information it has in its possession that it collected pursuant to their written contract with the business, or by enabling the business to access that personal information.

(j) In responding to a consumer's verified request to know categories of personal information, categories of sources, and/or categories of third parties, a business shall provide an individualized response to the consumer as required by the CCPA. It shall not refer the consumer to the businesses' information practices outlined in its privacy policy unless its response would be the same for all consumers and the privacy policy discloses all the information that is otherwise required to be in a response to a request to know such categories.

(k) In responding to a verified request to know categories of personal information, the business shall provide all of the following:

(1) The categories of personal information the business has collected about the consumer.

(2) The categories of sources from which the personal information was collected.

(3) The business or commercial purpose for which it collected or sold the personal information.

(4) The categories of third parties with whom the business shares personal information.

(5) The categories of personal information that the business sold, and for each category identified, the categories of third parties to whom it sold that particular category of personal information.

(6) The categories of personal information that the business disclosed for a business purpose, and for each category identified, the categories of third parties to whom it disclosed that particular category of personal information.

(l) A business shall identify the categories of personal information, categories of sources of personal information, and categories of third parties to whom a business sold or disclosed personal information, in a manner that provides consumers a meaningful understanding of the categories listed.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.110, 1798.115, 1798.130, 1798.140 and 1798.185, Civil Code.

11 C.F.R. § 7025. Opt-out Preference Signals

(a) The purpose of an opt-out preference signal is to provide consumers with a simple and easyto-use method by which consumers interacting with businesses online can automatically exercise their right to opt-out of sale/sharing. Through an opt-out preference signal, a consumer can opt-out of sale and sharing of their personal information with all businesses they interact with online without having to make individualized requests with each business.

(b) A business that sells or shares personal information shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing:

(1) The signal shall be in a format commonly used and recognized by businesses. An example would be an HTTP header field or JavaScript object.

(2) The platform, technology, or mechanism that sends the opt-out preference signal shall make clear to the consumer, whether in its configuration or in disclosures to the public, that the use of the signal is meant to have the effect of opting the consumer out of the sale and sharing of their personal information. The configuration or disclosure does not need to be tailored only to California or to refer to California.

(c) When a business that collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b):

(1) The business shall treat the opt-out preference signal as a valid request to opt-out of sale/sharing submitted pursuant to Civil Code section 1798.120 for that browser or device and any consumer profile associated with that browser or device, including pseudonymous profiles. If known, the business shall also treat the opt-out preference signal as a valid request to opt-out of sale/sharing for the consumer. This is not required for a business that does not sell or share personal information.

(2) The business shall not require a consumer to provide additional information beyond what is necessary to send the signal. However, a business may provide the consumer with an option to provide additional information if it will help facilitate the consumer's request to opt-out of sale/sharing. Any information provided by the consumer shall not be used, disclosed, or retained for any purpose other than processing the request to optout of sale/sharing. For example, a business may give the consumer the option to provide information that identifies the consumer so that the request to opt-out of sale/sharing can apply to offline sale or sharing of personal information. However, if the consumer does not respond, the business shall still process the opt-out preference signal as a valid request to opt-out of sale/sharing for that browser or device and any consumer profile the business associates with that browser or device, including pseudonymous profiles.

(3) If the opt-out preference signal conflicts with a consumer's business-specific privacy setting that allows the business to sell or share their personal information, the business shall process the opt-out preference signal as a valid request to opt-out of sale/sharing, but may notify the consumer of the conflict and provide the consumer with an opportunity to consent to the sale or sharing of their personal information. The business shall comply with section 7004 in obtaining the consumer's consent to the sale or sharing of their personal information. If the consumer consents to the sale or sharing of their personal information, the business may ignore the opt-out preference signal for as long as the consumer is known to the business.

(4) If the opt-out preference signal conflicts with the consumer's participation in a business's financial incentive program that requires the consumer to consent to the sale or sharing of personal information, the business may notify the consumer that processing the opt-out preference signal as a valid request to opt-out of sale/sharing would withdraw the consumer from the financial incentive program and ask the consumer to affirm that they intend to withdraw from the financial incentive program. If the consumer affirms that they intend to withdraw from the financial incentive program, the business shall process the consumer's request to opt-out of sale/sharing. If the business asks and the consumer does not affirm their intent to withdraw, the business may ignore the opt-out preference signal with respect to that consumer's participation in the financial incentive program for as long as the consumer is known to the business. If the

business does not ask the consumer to affirm their intent with regard to the financial incentive program, the business shall still process the opt-out preference signal as a valid request to opt-out of sale/sharing for that browser or device and any consumer profile the business associates with that browser or device.

(5) Where the consumer is known to the business, the business shall not interpret the absence of an opt-out preference signal after the consumer previously sent an opt-out preference signal as consent to opt-in to the sale or sharing of personal information.

(6) A business may display whether it has processed the consumer's opt-out preference signal as a valid request to opt-out of sale/sharing on its website. For example, the business may display on its website "Opt-Out Preference Signal Honored" when a browser, device, or consumer using an opt-out preference signal visits the website, or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.

(7) Illustrative examples follow.

(A) Caleb visits Business N's website using a browser with an opt-out preference signal enabled, but he is not otherwise logged into his account and the business cannot otherwise associate Caleb's browser with a consumer profile the business maintains. Business N collects and shares Caleb's personal information tied to his browser identifier for cross-context behavioral advertising. Upon receiving the opt-out preference signal, Business N shall stop selling and sharing Caleb's information linked to Caleb's browser identifier for cross-context behavioral advertising, but it would not be able to apply the request to opt-out of the sale/sharing to Caleb's account information because the connection between Caleb's browser and Caleb's account is not known to the business.

(B) Noelle has an account with Business O, an online retailer who manages consumer's privacy choices through a settings menu. Noelle's privacy settings default to allowing Business O to sell and share her personal information with the business's marketing partners. Noelle enables an opt-out preference signal on her browser and then visits Business O's website. Business O recognizes that Noelle is visiting its website because she is logged into her account. Upon receiving Noelle's opt-out preference signal, Business O shall treat the signal as a valid request to opt-out of sale/sharing and shall apply it to her device and/or browser and also to her account and any offline sale or sharing of personal information. Business O may inform Noelle that her opt-out preference signal differs from her current privacy settings and provide her with an opportunity to consent to the sale or sharing of her personal information, but it must process the request to opt-out of sale/sharing unless Noelle instructs otherwise. Business O must also wait at least 12 months before asking Noelle to opt-in to the sale or sharing of her personal information in accordance with section 7026, subsection (k). In addition, Business O's notification would not allow it to fall within the exception set forth in Civil Code section 1798.135, subdivision (b)(1), because it would not be complying with the requirements set forth in subsection (f).

(C) Angela also has an account with Business O and has enabled an opt-out preference signal on her browser while logged into her account. Business O applies the opt-out preference signal as a valid request to opt-out of sale/sharing not only to Angela's current browser, but also to Angela's account because she is known to the business while making the request. Angela later logs into her account with Business O using a different device that does not have the opt-out preference signal enabled. Business O shall not interpret the absence of the optout preference signal as consent to opt-in to the sale of personal information.

(D) Ramona participates in Business P's financial incentive program where she receives coupons in exchange for allowing the business to pseudonymously track and share her online browsing habits with marketing partners. Ramona enables an opt-out preference signal on her browser and then visits Business P's website. Business P knows that it is Ramona through a cookie that has been placed on her browser, but also detects the opt-out preference signal. Business P may ignore the opt-out preference signal and notify Ramona that her opt-out preference signal conflicts with her participation in the financial incentive program and ask whether she intends to withdraw from the financial incentive program. If Ramona does not affirm her intent to withdraw, Business P may ignore the opt-out preference signal and place Ramona on a whitelist so that Business P does not have to notify Ramona of the conflict again.

(E) Ramona clears her cookies and revisits Business P's website with the opt-out preference signal enabled. Business P no longer knows that it is Ramona visiting its website. Business P shall honor Ramona's opt-out preference signal as it pertains to her browser or device and any consumer profile the business associates with that browser or device.

(d) The business and the platform, technology, or mechanism that sends the opt-out preference signal shall not use, disclose, or retain any personal information collected from the consumer in connection with the sending or processing the request to opt-out of sale/sharing for any purpose other than sending or processing the opt-out preference signal.

(e) Civil Code section 1798.135, subdivisions (b)(1) and (3), provide a business the choice between (1) processing opt-out preference signals and providing the "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links or the Alternative Opt-out Link; or (2) processing opt-out preference signals in a frictionless manner in accordance with these regulations and not having to provide the "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links or the Alternative Opt-out Link. They do not give the business the choice between posting the above-referenced links or honoring opt-out preference signals. Even if the business posts the above-referenced links, the business must still process opt-out preference signals, though it may do so in a non-frictionless manner. If a business processes opt-out preference signals in a frictionless manner in accordance with subsections (f) and (g), then it may, but is not required to, provide the above-referenced links.

(f) Except as allowed by these regulations, processing an opt-out preference signal in a frictionless manner as required by Civil Code section 1798.135, subdivision (b)(1), means that the business shall not:

(1) Charge a fee or require any valuable consideration if the consumer uses an opt-out preference signal.

(2) Change the consumer's experience with the product or service offered by the business. For example, the consumer who uses an opt-out preference signal shall have the same experience with regard to how the business's product or service functions compared to a consumer who does not use an opt-out preference signal.

(3) Display a notification, pop-up, text, graphic, animation, sound, video, or any interstitial content in response to the opt-out preference signal. However, a business's display of whether the consumer visiting their website has opted out of the sale or sharing their personal information shall not be considered a violation of this regulation. The business may also provide a link to a privacy settings page, menu, or similar interface that enables the consumer to consent to the business ignoring the opt-out preference signal with respect to the business's sale or sharing of the consumer's personal information provided that it complies with subsections (f)(1) through (3).

(g) A business meeting the requirements of Civil Code section 1798.135, subdivision (b)(1) is not required to post the "Do Not Sell or Share My Personal Information" link or the Alternative Opt-out Link if it meets all of the following additional requirements:

(1) Processes the opt-out preference signal in a frictionless manner in accordance with the CCPA and these regulations.

(2) Includes in its privacy policy the following information:

(A) A description of the consumer's right to opt-out of the sale or sharing of their personal information by the business;

(B) A statement that the business processes opt-out preference signals in a frictionless manner;

(C) Information on how consumers can implement opt-out preference signals for the business to process in frictionless manner;

(D) Instructions for any other method by which the consumer may submit a request to opt-out of sale/sharing.

(3) Allows the opt-out preference signal to fully effectuate the consumer's request to optout of sale/sharing. For example, if the business sells or shares personal information offline and needs to request from the consumer additional information that is not provided by the opt-out preference signal in order to apply the request to opt-out of sale/sharing to offline sales and sharing of personal information, then the business has not fully effectuated the consumer's request to opt-out of sale/sharing. Illustrative examples follow.

(A) Business Q collects consumers' online browsing history and shares it with third parties for cross-context behavioral advertising purposes. Business Q also sells consumers' personal information offline to marketing partners. Business Q cannot fall within the exception set forth in Civil Code section 1798.135, subdivision (b)(1), because a consumer's opt-out preference signal would only apply to Business Q's online sharing of personal information about the consumer's browser or device; the consumer's opt-out preference signal would not apply to Business Q's offline selling of the consumer's information because Business Q could not apply it to the offline selling without additional information provided by the consumer, i.e., the logging into an account.

(B) Business R only sells and shares personal information online for cross-context behavioral advertising purposes. Business R may use the exception set forth in Civil Code section 1798.135, subdivision (b)(1), and not post the "Do Not Sell or Share My Personal Information" link because a consumer using an opt-out preference signal would fully effectuate their right to opt-out of the sale or sharing of their personal information.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, 1798.140 and 1798.185, Civil Code.

11 C.F.R. § 7026. Requests to Opt-Out of Sale/Sharing

(a) A business that sells or shares personal information shall provide two or more designated methods for submitting requests to opt-out of sale/sharing. A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the personal information that it makes available to third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of sale/sharing. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer.

(b) A business's methods for submitting requests to opt-out of sale/sharing shall be easy for consumers to execute, and shall require minimal steps, and shall comply with section 7004.

(c) A business shall not require a consumer submitting a request to opt-out of sale/sharing to create an account or provide additional information beyond what is necessary to direct the business not to sell or share the consumer's personal information.

(d) A business shall not require a verifiable consumer request for a request to opt-out of sale/sharing. A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer whose information shall cease to be sold or shared by the business. However, to the extent that the business can comply with a request to opt-out of sale/sharing without additional information, it shall do so.

(e) If a business has a good-faith, reasonable, and documented belief that a request to opt-out of sale/sharing is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request and shall provide to the requestor an explanation why it believes the request is fraudulent.

(f) A business shall comply with a request to opt-out of sale/sharing by:

(1) Ceasing to sell to and/or share with third parties the consumer's personal information as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. Service providers or contractors Collecting personal information pursuant to the written contract with the business required by the CCPA and these regulations does not constitute a sale or sharing of personal information.

(2) Notifying all third parties to whom the business has sold or shared the consumer's personal information, after the consumer submits the request to opt-out of sale/sharing and before the business complies with that request, that the consumer has made a request to opt-out of sale/sharing and directing them to comply with the consumer's request and forward the request to any other person to whom the third party has made the personal information available during that time period.

(g) A business may provide Providing a means by which the consumer can confirm that their request to opt-out of sale/sharing has been processed by the business. For example, the business may display on its website "Consumer Opted Out of Sale/Sharing" or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.

(h) In responding to a request to opt-out of sale/sharing, a business may present the consumer with the choice to opt-out of the sale or sharing of personal information for certain uses as long as a single option to opt-out of the sale or sharing of all personal information is also offered. However, doing so in response to an opt-out preference signal will prevent the business from using the exception set forth in Civil Code section 1798.135, subdivision (b)(1).

(i) A business that responds to a request to opt-out of sale/sharing by informing the consumer of a charge for the use of any product or service shall comply with Article 7 and shall provide the consumer with a Notice of Financial incentive that complies with section 7016 in its response. However, doing so in response to an opt-out preference signal will prevent the business from using the exception set forth in Civil Code section 1798.135, subdivision (b)(1).

(j) A consumer may use an authorized agent to submit a request to opt-out of sale/sharing on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent cannot does not provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf. The requirement to obtain and provide written permission from the consumer does not apply to requests made by an opt-out preference signal.

(k) Except as allowed by these regulations, a business shall wait at least 12 months from the date the consumer's request before asking a consumer who has opted out of the sale or sharing of their personal information to consent to the sale or sharing of their personal information.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, 1798.140 and 1798.185, Civil Code.

11 C.F.R. § 7027. Requests to Limit Use and Disclosure of Sensitive Personal Information

(a) The unauthorized use or disclosure of sensitive personal information creates a heightened risk of harm for the consumer. The purpose of the request to limit is to give consumers meaningful control over how their sensitive personal information is collected, used, and disclosed. It gives the consumer the ability to limit the business's use of sensitive personal information to that which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services, with some narrowly tailored exceptions, which are set forth in subsection (m). Sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to requests to limit.

(b) A business that uses or discloses sensitive personal information for purposes other than those set forth in subsection (m) shall provide two or more designated methods for submitting requests to limit. A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the sensitive personal information that it uses for purposes other than those set forth in subsection (m), available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to limit. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. Illustrative examples follow.

(1) A business that collects sensitive personal information from consumers online shall, at a minimum, allow consumers to submit requests to limit through an interactive form accessible via the "Limit the Use of My Sensitive Personal Information" link or the Alternative Opt-out Link.

(2) A business that interacts with consumers in person and online may provide an inperson method for submitting requests to limit in addition to the online form.

(3) Other methods for submitting requests to limit include, but are not limited to, a tollfree phone number, a designated email address, a form submitted in person, and a form submitted through the mail.

(4) A notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to limit because cookies concern the collection of personal information and not necessarily the use and disclosure of sensitive personal information. An acceptable method for submitting requests to limit must address the specific right to limit.

(c) A business's methods for submitting requests to limit shall be easy for consumers to execute, shall require minimal steps, and shall comply with section 7004.

(d) A business shall not require a consumer submitting a request to limit to create an account or provide additional information beyond what is necessary to direct the business to limit the use or disclosure of the consumer's sensitive personal information.

(e) A business shall not require a verifiable consumer request for a request to limit. A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer to whom the request should be applied. However, to the extent that the business can comply with a request to limit without additional information, it shall do so.

(f) If a business has a good-faith, reasonable, and documented belief that a request to limit is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request and shall provide to the requestor an explanation why it believes the request is fraudulent.

(g) A business shall comply with a request to limit by:

(1) Ceasing to use and disclose the consumer's sensitive personal information for purposes other than those set forth in subsection (m) as soon as feasibly possible, but no later than 15 business days from the date the business receives the request.

(2) Notifying all the business's service providers or contractors that use or disclose the consumer's sensitive personal information for purposes other than those set forth in subsection (m) that the consumer has made a request to limit and instructing them to comply with the consumer's request to limit within the same time frame.

(3) Notifying all third parties to whom the business has disclosed or made available the consumer's sensitive personal information for purposes other than those set forth in subsection (m), after the consumer submitted their request and before the business complies with that request, that the consumer has made a request to limit and direct them 1) to comply with the consumer's request and 2) to forward the request to any other person with whom the third party has disclosed or shared the sensitive personal information during that time period.

(h) A business may provide a means by which the consumer can confirm that their request to limit has been processed by the business. For example, the business may display through a toggle or radio button that the consumer has limited the business's use and disclosure of their sensitive personal information.

(i) In responding to a request to limit, a business may present the consumer with the choice to allow specific uses for the sensitive personal information as long as a single option to limit the use of the personal information is also offered.

(j) A consumer may use an authorized agent to submit a request to limit on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent does not provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf.

(k) A business that responds to a request to limit by informing the consumer of a charge for the use of any product or service shall comply with Article 7 and shall provide the consumer with a Notice of Financial Incentive that complies with section 7016 in its response.

(l) Except as allowed by these regulations, a business shall wait at least 12 months from the date the consumer's request to limit is received before asking a consumer who has exercised their right to limit to consent to the use or disclosure of their sensitive personal information for purposes other than those set forth in subsection (m).

(m) The purposes identified in Civil Code section 1798.121, subdivision (a), for which a business may use or disclose sensitive personal information without being required to offer consumers a right to limit are as follows. A business that only uses or discloses sensitive personal information for these purposes, provided that the use or disclosure is reasonably necessary and proportionate for those purposes, is not required to post a Notice of Right to Limit or provide a method for submitting a request to limit.

(1) To perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services. For example, a consumer's precise geolocation may be used by a mobile application that is providing the consumer with directions on how to get to a specific location. A consumer's precise geolocation may not, however, be used by a gaming application where the average consumer would not expect the application to need this piece of sensitive personal information.

(2) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information. For example, a business may disclose a consumer's log-in information to a data security company that it has hired to investigate and remediate a data breach that involved that consumer's account.

(3) To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions. For example, a business may use information about a consumer's ethnicity and/or the contents of email and text messages to investigate claims of racial discrimination or hate speech.

(4) To ensure the physical safety of natural persons. For example, a business may disclose a consumer's geolocation information to law enforcement to investigate an alleged kidnapping.

(5) For short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business, provided that the personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business. For example, a business that sells religious books can use information about its customers' interest in its religious content to serve contextual advertising for other kinds of religious merchandise within its store or on its website, so long as the business does not use sensitive personal information to create a profile about an individual consumer or disclose personal information that reveals consumers' religious beliefs to third parties.

(6) To perform services on behalf of the business. For example, a business may use information for maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.

(7) To verify or maintain the quality or safety of a product, service, or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured by, manufactured for, or controlled by the business. For example, a car rental business may use a consumer's driver's license for the purpose of testing that its internal text recognition software accurately captures license information used in car rental transactions.

(8) To collect or process sensitive personal information where the collection or processing is not for the purpose of inferring characteristics about a consumer. For example, a business that includes a search box on their website by which consumers can search for articles related to their health condition may use the information provided by the consumer for the purpose of providing the search feature without inferring characteristics about the consumer.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.121, 1798.135, 1798.140 and 1798.185, Civil Code.

11 C.F.R. § 7028. Requests to Opt-In After Opting-Out of the Sale or Sharing of Personal Information

(a) Requests to opt-in to sale or sharing of personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.

(b) If a consumer who has opted-out of the sale or sharing of their personal information initiates a transaction or attempts to use a product or service that requires the sale or sharing of their personal information, the business may inform the consumer that the transaction, product, or service requires the sale of their personal information and provide instructions on how the consumer can provide consent to opt-in to the sale or sharing of their personal information. The business shall comply with section 7004 when obtaining the consumer's consent.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

Article 4. SERVICE PROVIDERS, CONTRACTORS, AND THIRD PARTIES

11 C.F.R. § 7050. Service Providers and Contractors

(a) A service provider or contractor shall not retain, use, or disclose personal information collected pursuant to its written contract with the business obtained in the course of providing services except:

(1) For the specific business purpose(s) set forth in the written contract between the business and the service provider or contractor that is required by the CCPA and these regulations.;

(2) To retain and employ another service provider or contractor as a subcontractor, where the subcontractor meets the requirements for a service provider or contractor under the CCPA and these regulations.;

(3) For internal use by the service provider or contractor to build or improve the quality of the services it is providing to the business, even if this business purpose is not specified in the written contract required by the CCPA and these regulations, provided that the service provider or contractor does not use the personal information to perform services on behalf of another person. Illustrative examples follow.

(A) An email marketing service provider can send emails on a business's behalf using the business's customer email list. The service provider could analyze those customers' interactions with the marketing emails to improve its services and offer those improved services to everyone. But the service provider cannot use the original email list to send marketing emails on behalf of another business.

(B) A shipping service provider that delivers businesses' products to their customers may use the addresses received from their business clients and their experience delivering to those addresses to identify faulty or incomplete addresses, and thus, improve their delivery services. However, the shipping service provider cannot compile the addresses received from one business to send advertisements on behalf of another business, or compile addresses received from businesses to sell to data brokers.

(4) To prevent, detect, or investigate data security incidents or protect against malicious, deceptive, fraudulent or illegal activity, even if this business purpose is not specified in the written contract required by the CCPA and these regulations.;

(5) For the purposes enumerated in Civil Code section 1798.145, subdivisions (a)(1) through (a)(74).

(b) A service provider or contractor cannot contract with a business to provide cross-context behavioral advertising. Pursuant to Civil Code section 1798.140, subdivision (e)(6), a service provider or contractor may contract with a business to provide advertising and marketing services, but the service provider or contractor shall not combine the personal information of consumers who have opted-out of the sale/sharing that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or collects from its own interaction with consumers. A person who contracts with a business to provide cross-context behavioral advertising is a third party and not a service provider or contractor with respect to cross-context behavioral advertising services. Illustrative examples follow.

(1) Business S, a clothing company, hires a social media company as a service provider for the purpose of providing Business S's advertisements on the social media company's platform. The social media company can serve Business S by providing non-personalized advertising services on its platform based on aggregated or demographic information (e.g., advertisements to women, 18-30 years old, that live in Los Angeles). However, it cannot use a list of customer email addresses provided by Business S to identify users on the social media company's platform to serve advertisements to them.

(2) Business T, a company that sells cookware, hires an advertising company as a service provider for the purpose of advertising its services. The advertising agency can serve Business T by providing contextual advertising services, such as placing advertisements for Business T's products on websites that post recipes and other cooking tips.

(c) If a service provider or contractor receives a request made pursuant to the CCPA directly from the consumer, the service provider or contractor shall either act on behalf of the business in accordance with the business's instructions for responding to the request or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider or contractor.

(d) A service provider or contractor that is a business shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider or contractor.

(e) A person who does not have a contract that complies with section 7051, subsection (a), is not a service provider or a contractor under the CCPA. For example, a business's disclosure of personal information to a person who does not have a contract that complies with section 7051, subsection (a), may be considered a sale or sharing of personal information for which the business must provide the consumer with the right to opt-out of sale/sharing.

(f) A service provider or a contractor shall comply with the terms of the contract required by the CCPA and these regulations.

(g) Whether an entity that provides services to a nonbusiness must comply with a consumer's CCPA request depends upon whether the entity is a "business," as defined by Civil Code section 1798.140, subdivision (d).

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.

11 C.F.R. § 7051. Contract Requirements for Service Providers and Contractors

(a) The contract required by the CCPA for service providers and contractors shall:

(1) Prohibit the service provider or contractor from selling or sharing personal information business it Collects pursuant to the written contract with the business.

(2) Identify the specific Business Purpose(s) for which the service provider or contractor is processing personal information pursuant to the written contract with the business, and specify that the business is disclosing the personal information to the service provider or contractor only for the limited and specified Business Purpose(s) set forth within the contract. The Business Purpose shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.

(3) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it Collected pursuant to the written contract with the business for any purposes other than the Business Purpose(s) specified in the contract or as otherwise permitted by the CCPA and these regulations.

(4) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it Collected pursuant to the written contract with the business for any commercial purpose other than the Business Purposes specified in the contract, unless expressly permitted by the CCPA or these regulations.

(5) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it Collected pursuant to the written contract with the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. For example, a service provider or contractor shall be prohibited from combining or updating personal information that it Collected pursuant to the written contract with the business with personal information that it received from another source or Collected from its own interaction with the consumer, unless expressly permitted by the CCPA or these regulations.

(6) Require the service provider or contractor to comply with all applicable sections of the CCPA and these regulations, including—with respect to the personal information that it Collected pursuant to the written contract with the business—providing the same level of privacy protection as require of businesses by the CCPA and these regulations. For example, the contract may require the service provider or contractor to cooperate with the business in responding to and complying with consumers' requests made pursuant to the CCPA, and to implement reasonable security procedures and practices appropriate to the nature of the personal information the business to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.

(7) Grant the business the right to take reasonable and appropriate steps to ensure that service provider or contractor uses the personal information that it Collected pursuant to the written contract with the business in a manner consistent with the business's obligations under the CCPA and these regulations. Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider's system and regular internal or third-party assessments, audits, or other technical and operational testing at least once every 12 months.

(8) Require the service provider or contractor to notify the business after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.

(9) Grant the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate the service provider or contractor's unauthorized use of personal information. For example, the business may require the service provider or contractor to provide documentation that verifies that they no longer retain or use the personal information of consumers that have made a valid request to delete with the business.

(10) Require the service provider or contractor to enable the business to comply with consumer requests made pursuant to the CCPA or require the business to inform the service provider or contractor of any consumer request made pursuant to the CCPA that they must comply with and provide the information necessary for the service provider or contractor to comply with the request.

(b) A service provider or contractor that subcontracts with another person in providing services to the business for whom it is a service provider or contractor shall have a contract with the subcontractor that complies with the CCPA and these regulations, including subsection (a).

(c) Whether a business conducts due diligence of its service providers and contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract nor exercises its rights to audit or test the service provider's or contractor's systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the service provider or contractor.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.

11 C.F.R. § 7052. Third Parties

(a) A third party that does not have a contract that complies with section 7053, subsection (a), shall not collect, use, process, retain, sell, or share the personal information that the business made available to it.

(b) A third party shall comply with the terms of the contract required by the CCPA and these regulations, which include treating the personal information that the business made available to it in a manner consistent with the business's obligations under the CCPA and these regulations.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.

11 C.F.R. § 7053. Contract Requirements for Third Parties

(a) A business that sells or shares a consumer's personal information with a third party shall enter into an agreement with the third party that:

(1) Identifies the limited and specified purpose(s) for which the personal information is made available to the third party. The purpose(s) shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.

(2) Specifies that the business is making the personal information available to the third party only for the limited and specified purpose(s) set forth within the contract and requires the third party to use it only for that limited and specified purpose(s).

(3) Requires the third party to comply with all applicable sections of the CCPA and these regulations, including—with respect to the personal information that the business makes available to the third party—providing the same level of privacy protection as required of businesses by the CCPA and these regulations. For example, the contract may require the third party to comply with a consumer's request to opt-out of sale/sharing forwarded to it by a first-party business and to implement reasonable security procedures and practices appropriate to the nature of the personal information

to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.

(4) Grants the business the right—with respect to the personal information that the business makes available to the third party—to take reasonable and appropriate steps to ensure that the third party uses it in a manner consistent with the business's obligations under the CCPA and these regulations. For example, the business may require the third party to attest that it treats the personal information the business made available to it in the same manner that the business is obligated to treat it under the CCPA and these regulations.

(5) Grants the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information made available to the third party. For example, the business may require the third party to provide documentation that verifies that it no longer retains or uses the personal information of consumers who have had their requests to opt-out of sale/sharing forwarded to it by the first party business.

(6) Requires the third party to notify the business after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.

(b) Whether a business conducts due diligence of the third party factors into whether the business has reason to believe that the third party is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract might not be able to rely on the defense that it did not have reason to believe that the third party intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the third party.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.

Article 5. VERIFICATION OF REQUESTS

11 C.F.R. § 7060. General Rules Regarding Verification

(a) A business shall establish, document, and comply with a reasonable method for verifying that the person making a request to know or a request to delete, request to correct, or request to know is the consumer about whom the business has collected information.

(b) A business shall not require a consumer to verify their identity to make a request to opt-out of sale/sharing or to make a request to limit. A business may ask the consumer for information necessary to complete the request; however, it shall not be burdensome on the consumer. For example, a business may ask the consumer for their name, but it shall not require the consumer to take a picture of themselves with their driver's license.

(c) In determining the method by which the business will verify the consumer's identity, the business shall:

(1) Whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business, or use a third-party identity verification service that complies with this section.

(2) Avoid collecting the types of personal information identified in Civil Code section 1798.81.5, subdivision (d), unless necessary for the purpose of verifying the consumer.

(3) Consider the following factors:

(A) The type, sensitivity, and value of the personal information collected and maintained about the consumer. Sensitive or valuable personal information shall warrant a more stringent verification process.

(B) The risk of harm to the consumer posed by any unauthorized deletion, correction, or access. A greater risk of harm to the consumer by unauthorized deletion, correction, or access shall warrant a more stringent verification process.;

(C) The likelihood that fraudulent or malicious actors would seek the personal information. The higher the likelihood, the more stringent the verification process shall be.;

(D) Whether the personal information to be provided by the consumer to verify their identity is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated.

(E) The manner in which the business interacts with the consumer.;

(F) Available technology for verification.

(d) A business shall generally avoid requesting additional information from the consumer for purposes of verification. If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, security, or fraud-prevention. The business shall delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer's request, except as required to comply with section 7101.

(e) A business shall not require the consumer or the consumer's authorized agent to pay a fee for the verification of their request to delete, request to correct, or request to know. For example, a business may not require a consumer to provide a notarized affidavit to verify their identity unless the business compensates the consumer for the cost of notarization.

(f) A business shall implement reasonable security measures to detect fraudulent identity verification activity and prevent the unauthorized or deletion, correction, or access of a consumer's personal information.

(g) If a business maintains consumer information that is deidentified, a business is not obligated to provide or delete this information in response to a consumer request or to reidentify individual data to verify a consumer request.

(h) For requests to correct, the business shall make an effort to verify the consumer based on personal information that is not the subject of the request to correct. For example, if the consumer is contending that the business has the wrong address for the consumer, the business shall not use address as a means of verifying the consumer's identity.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.

11 C.F.R. § 7061. Verification for Password-Protected Accounts

(a) If a business maintains a password-protected account with the consumer, the business may verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the business follows the requirements in section 7060. The business shall also require a consumer to re-authenticate themselves before deleting, correcting, or disclosing the consumer's data.

(b) If a business suspects fraudulent or malicious activity on or from the password-protected account, the business shall not comply with a consumer's request to delete, request to correct, or request to know until further verification procedures determine that the consumer request is authentic and the consumer making the request is the person about whom the business has collected information. The business may use the procedures set forth in section 7062 to further verify the identity of the consumer.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code.

11 C.F.R. § 7062. Verification for Non-Accountholders

(a) If a consumer does not have or cannot access a password-protected account with a business, the business shall comply with this section, in addition to section 7060.

(b) A business's compliance with a request to know categories of personal information requires that the business verify the identity of the consumer making the request to a reasonable degree of certainty. A reasonable degree of certainty may include matching at least two data points provided by the consumer with data points maintained by the business that it has determined to be reliable for the purpose of verifying the consumer.

(c) A business's compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. If a business uses this method for verification, the business shall maintain all signed declarations as part of its record-keeping obligations.

(d) A business's compliance with a request to delete or a request to correct may require that the business verify the identity of the consumer to a reasonable or reasonably high degree of certainty depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion or correction. For example, the deletion of family photographs or the correction of contact information may require a reasonably high degree of certainty, while the deletion of browsing history or correction of marital status may require only a reasonable degree of certainty. A business shall act in good faith when determining the appropriate standard to apply when verifying the consumer in accordance with these regulations.

(e) Illustrative examples follow:

(1) *Example 1*: If a business maintains personal information in a manner associated with a named actual person, the business may verify the consumer by requiring the consumer to provide evidence that matches the personal information maintained by the business. For example, if a retailer maintains a record of purchases made by a consumer, the business may require the consumer to identify items that they recently purchased from the store or the dollar amount of their most recent purchase to verify their identity to a reasonable degree of certainty.

(2) *Example 2*: If a business maintains personal information in a manner that is not associated with a named actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the personal information. For example, a business may have a mobile application that collects personal information about the consumer but does not require an account. The business may determine whether, based on the facts and considering the factors set forth in section 7060, subsection (b)(3), it may reasonably verify a consumer by asking them to provide information that only the person who used the mobile application may know or by requiring the consumer to respond to a notification sent to their device.

(f) A business shall deny a request to know specific pieces of personal information if it cannot verify the identity of the requestor pursuant to these regulations.

(g) If there is no reasonable method by which a business can verify the identity of the consumer to the degree of certainty required by this section, the business shall state so in response to any request and explain why it has no reasonable method by which it can verify the identity of the requestor. If the business has no reasonable method by which it can verify any consumer, the business shall explain why it has no reasonable verification method in its privacy policy. The business shall evaluate and document whether a reasonable method can be established at least once every 12 months, in connection with the requirement to update the privacy policy set forth in Civil Code section 1798.130, subdivision (a)(5).

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code.

11 C.F.R. § 7063. Authorized Agents

(a) When a consumer uses an authorized agent to submit a request to know or a request to delete, request to correct, or a request to know, a business may require the authorized agent to provide proof that the consumer gave the agent signed permission to submit the request. The business may also require the consumer to do either of the following:

(1) Verify their own identity directly with the business.

(2) Directly confirm with the business that they provided the authorized agent permission to submit the request.

(b) Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4121 to 4130. A business shall not require power of attorney in order for a consumer to use an authorized agent to act on their behalf.

(c) An authorized agent shall implement and maintain reasonable security procedures and practices to protect the consumer's information.

(d) An authorized agent shall not use a consumer's personal information, or any information collected from or about the consumer, for any purposes other than to fulfill the consumer's requests, verification, or fraud prevention.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code.

Article 6. SPECIAL RULES REGARDING CONSUMERS UNDER 16 YEARS OF AGE

11 C.F.R. § 7070. Consumer Less Than 13 Years of Age

(a) Process for Opting-In to Sale or Sharing of Personal Information

(1) A business that has actual knowledge that it sells or shares the personal information of a consumer less than the age of 13 shall establish, document, and comply with a reasonable method for determining that the person consenting to the sale or sharing of the personal information about the child is the parent or guardian of that child. This consent to the sale or sharing of personal information is in addition to any verifiable parental consent required under COPPA.

(2) Methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian include, but are not limited to:

(A) Providing a consent form to be signed by the parent or guardian under penalty of perjury and returned to the business by postal mail, facsimile, or electronic scan;

(B) Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;

(C) Having a parent or guardian call a toll-free telephone number staffed by trained personnel;

(D) Having a parent or guardian connect to trained personnel via video-conference;

(E) Having a parent or guardian communicate in person with trained personnel; and

(F) Verifying a parent or guardian's identity by checking a form of government issued identification against databases of such information, as long as the parent or guardian's identification is deleted by the business from its records promptly after such verification is complete.

(b) When a business receives an consent to the sale or sharing of personal information pursuant to subsection (a), the business shall inform the parent or guardian of the right to opt-out of sale/sharing and of the process for doing so on behalf of their child pursuant to section 7026, subsections (a)-(f).

(c) A business shall establish, document, and comply with a reasonable method, in accordance with the methods set forth in subsection (a)(2), for determining that a person submitting a request delete, request to correct, or request to know the personal information of a child under the age of 13 is the parent or guardian of that child.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

11 C.F.R. § 7071. Consumers at Least 13 Years of Age and Less than 16 Years of Age

(a) A business that has actual knowledge that it sells or shares the personal information of consumers at least 13 years of age and less than 16 years of age shall establish, document, and comply with a reasonable process for allowing such consumers to opt-in to the sale or sharing of their personal information, pursuant to section 7028.

(b) When a business receives a request to opt-in to the sale or sharing of personal information from a consumer at least 13 years of age and less than 16 years of age, the business shall inform the consumer of their ongoing right to opt-out of sale/sharing at any point in the future and of the process for doing so pursuant to section 7026.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

11 C.F.R. § 7072. Notices to Consumers Less Than 16 Years of Age

(a) A business subject to sections 7070 and/or 7071 shall include a description of the processes set forth in those sections in its privacy policy.

(b) A business that exclusively targets offers of goods or services directly to consumers under 16 years of age and does not sell or share the personal information without the consent of consumers at least 13 years of age and less than 16 years of age, or the consent of their parent or guardian for consumers under 13 years of age, is not required to provide the Notice of Right to Opt-out of Sale/Sharing.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

Article 7. NON-DISCRIMINATION

11 C.F.R. § 7080. Discriminatory Practices

(a) A price or service difference is discriminatory, and therefore prohibited by Civil Code section 1798.125, if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or these regulations.

(b) A business may offer a price or service difference that is nondiscriminatory. A price or service difference is non-discriminatory if it is reasonably related to the value of the consumer's data. If a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the price or service difference.

(c) A business's denial of a consumer's request to delete, request to correct, request to know, or request to opt-out of sale/sharing for reasons permitted by the CCPA or these regulations shall not be considered discriminatory.

(d) Illustrative examples follow:

(1) Example 1: A music streaming business offers a free service as well as a premium service that costs $5 per month. If only the consumers who pay for the music streaming service are allowed to opt-out of the sale or sharing of their personal information, then the practice is discriminatory, unless the $5-per-month payment is reasonably related to the value of the consumer's data to the business.

(2) Example 2: A clothing business offers a loyalty program whereby customers receive a $5-off coupon by email after spending $100 with the business. A consumer submits a request to delete all personal information the business has collected about them but also informs the business that they want to continue to participate in the loyalty program. The business may deny their request to delete with regard to their email address and the amount the consumer has spent with the business because that information is necessary for the business to provide the loyalty program requested by the consumer and is reasonably anticipated within the context of the business's ongoing relationship with them pursuant to Civil Code section 1798.105, subdivision (d)(1).

(3) Example 3: A grocery store offers a loyalty program whereby consumers receive coupons and special discounts when they provide their phone numbers. A consumer submits a request to opt-out of the sale/sharing of their personal information. The retailer complies with their request but no longer allows the consumer to participate in the loyalty program. This practice is discriminatory unless the grocery store can demonstrate that the value of the coupons and special discounts are reasonably related to the value of the consumer's data to the business.

(4) Example 4: An online bookseller collects information about consumers, including their email addresses. It offers coupons to consumers through browser pop-up windows while the consumer uses the bookseller's website. A consumer submits a request to delete all personal information that the bookseller has collected about them, including their email address and their browsing and purchasing history. The bookseller complies with the request but stops providing the periodic coupons to the consumer. The bookseller's failure to provide coupons is discriminatory unless the value of the coupons is reasonably related to the value provided to the business by the consumer's data. The bookseller may not deny the consumer's request to delete with regard to the email address because the email address is not necessary to provide the coupons or reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

(e) A business shall notify consumers of any financial incentive or price or service difference subject to Civil Code section 1798.125 that it offers in accordance with section 7016.

(f) A business's charging of a reasonable fee pursuant to Civil Code section 1798.145, subdivision (h)(3), shall not be considered a financial incentive subject to these regulations.

(g) A price or service difference that is the direct result of compliance with a state or federal law shall not be considered discriminatory.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125, 1798.130 and 1798.185, Civil Code.

11 C.F.R. § 7081. Calculating the Value of Consumer Data

(a) A business offering a price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good -faith method for calculating the value of the consumer's data. The business shall consider one or more of the following:

(1) The marginal value to the business of the sale, collection, or deletion of a consumer's data.

(2) The average value to the business of the sale, collection, or deletion of a consumer's data.

(3) The aggregate value to the business of the sale, collection, or deletion of consumers' data divided by the total number of consumers.

(4) Revenue generated by the business from sale, collection, or retention of consumers' personal information.

(5) Expenses related to the sale, collection, or retention of consumers' personal information.

(6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference.

(7) Profit generated by the business from sale, collection, or retention of consumers' personal information.

(8) Any other practical and reasonably reliable method of calculation used in good faith.

(b) For the purpose of calculating the value of consumer data, a business may consider the value to the business of the data of all natural persons in the United States and not just consumers.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125, 1798.130 and 1798.185, Civil Code.

Article 8. TRAINING AND RECORD-KEEPING

11 C.F.R. § 7100. Training

(a) All individuals responsible for handling consumer inquiries about the business's information practices or the business's compliance with the CCPA shall be informed of all of the requirements in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations.

(b) A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests made under the CCPA or the business's compliance with the CCPA are informed of all the requirements in these regulations and the CCPA.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130, 1798.135 and 1798.185, Civil Code.

11 C.F.R. § 7101. Record-Keeping

(a) A business shall maintain records of consumer requests made pursuant to the CCPA and how it responded to the requests for at least 24 months. The business shall implement and maintain reasonable security procedures and practices in maintaining these records.

(b) The records may be maintained in a ticket or log format provided that the ticket or log includes the date of request, nature of request, manner in which the request was made, the date of the business's response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part.

(c) A business's maintenance of the information required by this section, where that information is not used for any other purpose, does not taken alone violate the CCPA or these regulations.

(d) Information maintained for record-keeping purposes shall not be used for any other purpose except as reasonably necessary for the business to review and modify its processes for compliance with the CCPA and these regulations. Information maintained for record keeping purposes shall not be shared with any third party except as necessary to comply with a legal obligation.

(e) Other than as required by subsection (b), a business is not required to retain personal information solely for the purpose of fulfilling a consumer request made under the CCPA.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135 and 1798.185, Civil Code.

11 C.F.R. § 7102. Requirements for Businesses Collecting Large Amounts of Personal Information

(a) A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, shares, or otherwise makes available for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall:

(1) Compile the following metrics for the previous calendar year:

(A) The number of requests to delete that the business received, complied with in whole or in part, and denied;

(B) The number of requests to correct that the business received, complied with in whole or in part, and denied;

(C) The number of requests to know that the business received, complied with in whole or in part, and denied;

(D) The number of requests to opt-out of sale/sharing that the business received, complied with in whole or in part, and denied; and

(E) The number of requests to limit that the business received, complied with in whole or in part, and denied; and

(F) The median or mean number of days within which the business substantively responded to requests to know, requests to delete, requests to correct, requests to know, requests to opt-out of sale/sharing, and requests to opt-out limit.

(2) Disclose, by July 1 of every calendar year, the information compiled in subsection (a)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy. In its disclosure, a business may choose to disclose the number of requests that it denied in whole or in part because the request was not verifiable, was not made by a consumer, called for information exempt from disclosure, or was denied on other grounds.

(b) A business may choose to compile and disclose the information required by subsection (a)(1) for requests received from all individuals, rather than requests received from consumers. The business shall state whether it has done so in its disclosure and shall, upon request, compile and provide to the Attorney General the information required by subsection (a)(1) for requests received from consumers.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135 and 1798.185, Civil Code.

ARTICLE 9. INVESTIGATIONS AND ENFORCEMENT

11 C.F.R. § 7300. Sworn Complaints Filed with the Agency

(a) Requirements for filing a sworn complaint. Sworn complaints may be filed with the Enforcement Division via the electronic complaint system available on the Agency's website at https://cppa.ca.gov/ or submitted in person or by mail to the headquarters office of the Agency. A complaint must:

(1) Identify the business, service provider, contractor, or person who allegedly violated the CCPA;

(2) State the facts that support each alleged violation and include any documents or other evidence supporting this conclusion;

(3) Authorize the alleged violator and the Agency to communicate regarding the complaint, including disclosing the complaint and any information relating to the complaint;

(4) Include the name and current contact information of the complainant; and

(5) Be signed and submitted under penalty of perjury.

(b) The Enforcement Division will notify the complainant in writing of the action, if any, the Agency has taken or plans to take on the complaint, together with the reasons for that action or nonaction. Duplicate complaints submitted by the same complainant may be rejected without notice.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.199.45, Civil Code.

11 C.F.R. § 7301. Investigations

(a) The Agency may open investigations upon the sworn complaint of any person or on its own initiative. For example, the Agency may initiate investigations based upon referrals from government agencies or private organizations, and non-sworn or anonymous complaints.

(b) As part of the Agency's decision to pursue investigations of possible or alleged violations of the CCPA, the Agency may consider all facts it determines to be relevant, including the amount of time between the effective date of the statutory or regulatory requirement(s) and the possible or alleged violation(s) of those requirements, and good-faith efforts to comply with those requirements.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.199.45, Civil Code.

11 C.F.R. § 7302. Probable Cause Proceedings

(a) Probable Cause. Under Civil Code section 1798.199.50, probable cause exists when the evidence supports a reasonable belief that the CCPA has been violated.

(b) Probable Cause Notice. The Enforcement Division will provide the alleged violator with notice of the probable cause proceeding as required by Civil Code section 1798.199.50.

(c) Probable Cause Proceeding.

(1) The proceeding shall be closed to the public unless the alleged violator files, at least 10 business days before the proceeding, a written request for a public proceeding. If the proceeding is not open to the public, then the proceeding may be conducted in whole or in part by telephone or video-conference.

(2) The Agency shall conduct the proceeding informally. Only the alleged violator(s), their legal counsel, and the Enforcement Division shall have the right to participate at the proceeding. The Agency shall determine whether there is probable cause based on the probable cause notice and any information or arguments presented at the probable cause proceeding by the parties.

(3) If the alleged violator(s) fails to participate or appear at the probable cause proceeding, the alleged violator(s) waives the right to further probable cause proceedings under Civil Code section 1798.199.50, and the Agency shall determine whether there is probable cause based on the notice and any information or arguments provided by the Enforcement Division.

(d) Probable Cause Determination. The Agency shall issue a written decision with its probable cause determination and serve it on the alleged violator electronically or by mail. The Agency's probable cause determination is final and not subject to appeal.

(e) Notices of probable cause and probable cause determinations shall not be open to the public nor admissible in evidence in any action or special proceeding other than one enforcing the CCPA.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.199.50, Civil Code.

11 C.F.R. § 7303. Stipulated Orders

(a) At any time before or during an administrative hearing and in lieu of such a hearing, the Head of Enforcement and the alleged violator may stipulate to the entry of a final order. If a stipulation has been agreed upon and the scheduled date of the hearing is set to occur before the next Board meeting, the Enforcement Division will apply for a continuance of the hearing.

(b) The final order must be approved by the Board, which may consider the matter in closed session.

(c) The stipulated final order shall be public and have the force of an order of the Board.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.199.35 and 1798.199.55, Civil Code.

11 C.F.R. § 7304. Agency Audits

(a) Scope. The Agency may audit a business, service provider, contractor, or person to ensure compliance with any provision of the CCPA.

(b) Criteria for Selection. The Agency may conduct an audit to investigate possible violations of the CCPA. Alternatively, the Agency may conduct an audit if the subject's collection or processing of personal information presents significant risk to consumer privacy or security, or if the subject has a history of noncompliance with the CCPA or any other privacy protection law.

(c) Audits may be announced or unannounced as determined by the Agency.

(d) Failure to Cooperate. A subject's failure to cooperate during the Agency's audit may result in the Agency issuing a subpoena, seeking a warrant, or otherwise exercising its powers to ensure compliance with the CCPA.

(e) Protection of Personal Information. Consumer personal information disclosed to the Agency during an audit shall be maintained in compliance with the Information Practices Act of 1977, Civil Code section 1798, et seq.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.185, 1798.199.40 and 1798.199.65, Civil Code; Section 11180, Government Code.

Colorado Privacy Act

6-1-1301. Short title. The “Colorado Privacy Act”.

6-1-1302. Legislative declaration.

(1) The General Assembly hereby:

(a) finds that:

(I) the people of Colorado regard their privacy as a Fundamental right and an essential element of their individual freedom;

(II) Colorado’s constitution explicitly provides the right to privacy under section 7 of article ii, and fundamental privacy rights have long been, and continue to be, integral to protecting Coloradans and to safeguarding our democratic republic;

(III) ongoing advances in technology have produced exponential growth in the volume and variety of personal data being generated, collected, stored, and analyzed and these advances present both promise and potential peril;

(IV) the ability to harness and use data in positive ways is driving innovation and brings beneficial technologies to society, but it has also created risks to privacy and freedom; and

(V) the unauthorized disclosure of personal information and loss of privacy can have devastating impacts ranging from Financial fraud, identity theft, and unnecessary costs in personal time and finances to destruction of property, harassment, reputational damage, emotional distress, and physical harm;

(b) determines that:

(I) technological innovation and new uses of data can help solve societal problems and improve lives, and it is possible to build a world where technological innovation and privacy can coexist; and

(II) states across the United States are looking to this part 13 and similar models to enact state-based data privacy requirements and to exercise the leadership that is lacking at the national level; and

(c) declares that:

(I) by enacting this Part 13, Colorado will be among the states that empower consumers to protect their privacy and require companies to be responsible custodians of data as they continue to innovate;

(II) this Part 13 addresses issues of statewide concern and:

(A) provides consumers the right to access, correct, and delete personal data and the right to opt out not only of the sale of personal data but also of the collection and use of personal data;

(B) imposes an affirmative obligation upon companies to Safeguard personal data; to provide clear, understandable, and Transparent information to consumers about how their personal data are used; and to strengthen compliance and accountability by requiring data protection assessments in the collection and use of personal data; and

(C) empowers the attorney general and district attorneys to access and evaluate a company’s data protection assessments, to impose penalties where violations occur, and to prevent future violations.

6-1-1303. Definitions.

As used in this Part 13, unless the context otherwise requires:

(1) "Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity. As used in this subsection (1), "control" means:

(a) ownership of, control of, or power to vote twenty-five percent or more of the outstanding shares of any class of voting security of the entity, directly or indirectly, or acting through one or more other persons; Page 3-senate bill 21-190

(b) control in any manner over the election of a majority of the directors, trustees, or general partners of the entity or of individuals exercising similar functions; or

(c) the power to exercise, directly or indirectly, a controlling influence over the management or policies of the entity as determined by the applicable prudential regulator, as that term is defined in 12 U.S.C. SEC. 5481 (24), if any.

(2) "authenticate" means to use reasonable means to determine that a request to exercise any of the rights in section 6-1-1306 (1) is being made by or on behalf of the consumer who is entitled to exercise the rights.

(3) "Business Associate" has the meaning established in 45 Cfr 160.103.

(4) "Child" means an individual under thirteen years of age.

(5) "Consent" means a clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement, such as by a written statement, including by electronic means, or other clear, affirmative action by which the consumer signifies agreement to the processing of personal data. The following does not constitute consent:

(a) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information;

(b) hovering over, muting, pausing, or closing a given piece of content; and

(c) agreement obtained through dark patterns.

(6) "Consumer":

(a) means an individual who is a Colorado resident acting only in an individual or household context; and Page 4-senate bill 21-190

(b) does not include an individual acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context.

(7) "Controller" means a person that, alone or jointly with others, determines the purposes for and means of processing personal data.

(8) "Covered Entity" has the meaning established in 45 cfr 160.103.

(9) "Dark Pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice.

(10) "Decisions that produce legal or similarly significant effects concerning a consumer" means a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services.

(11) "De-identified Data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such an individual, if the controller that possesses the data:

(a) takes reasonable measures to ensure that the data cannot be associated with an individual;

(b) publicly commits to maintain and use the data only in a de-identified fashion and not attempt to re-identify the data; and

(c) contractually obligates any recipients of the information to comply with the requirements of this subsection (11).

(12) "Health-care Facility" means any entity that is licensed, certified, or otherwise authorized or permitted by law to administer medical treatment in this state.

(13) "Health-care Information" means individually identifiable information relating to the past, present, or future health status of an individual.

(14) "Health-care Provider" means a person licensed, certified, or registered in this state to practice medicine, pharmacy, chiropractic, nursing, physical therapy, podiatry, dentistry, optometry, occupational therapy, or other healing arts under title 12.

(15) "HIPAA" means the federal "health insurance portability and accountability act of 1996", as amended, 42 u.s.c. secs. 1320d to 1320d-9.

(16) "Identified or Identifiable Individual" means an individual who can be readily identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, specific geolocation data, or an online identifier.

(17) "Personal Data":

(a) means information that is linked or reasonably linkable to an identified or identifiable individual; and

(b) does not include de-identified data or publicly available information. As used in this subsection (17)(b), "publicly available information" means information that is lawfully made available from federal, state, or local government records and information that a controller has a reasonable basis to believe the consumer has lawfully made available to the general public.

(18) "Process" or "Processing" means the collection, use, sale, storage, disclosure, analysis, deletion, or modification of personal data and includes the actions of a controller directing a processor to process personal data.

(19) "Processor" means a person that processes personal page 6-senate bill 21-190 data on behalf of a controller.

(20) "Profiling" means any form of automated processing of personal data to evaluate, analyze, or predict personal spects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(21) "Protected Health Information" has the meaning established in 45 cfr 160.103.

(22) "Pseudonymous Data" means personal data that can no longer be attributed to a specific individual without the use of additional information if the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to a specific individual.

(23) (a) "Sale", "Sell", or "Sold" means the exchange of personal data for monetary or other valuable consideration by a controller to a third party.

(b) "Sale", "Sell", or "Sold" does not include the following:

(I) the disclosure of personal data to a processor that processes the personal data on behalf of a controller;

(II) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;

(III) the disclosure or transfer of personal data to an affiliate of the controller;

(IV) the disclosure or transfer to a third party of personal data as an asset that is part of a proposed or actual merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets; or

(V) the disclosure of personal data:

(A) that a consumer directs the controller to disclose or intentionally discloses by using the controller to interact with a third party; or

(B) intentionally made available by a consumer to the general public via a channel of mass media.

(24) "Sensitive Data" means:

(a) personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status;

(b) genetic or biometric data that may be processed for the purpose of uniquely identifying an individual; or

(c) personal data from a known child.

(25) "Targeted Advertising":

(a) means displaying to a consumer an advertisement that is selected based on personal data obtained or inferred over time from the consumer's activities across nonaffiliated websites, applications, or online services to predict consumer references or interests; and

(b) does not include:

(I) advertising to a consumer in response to the consumer's request for information or feedback;

(II) advertisements based on activities within a controller's own websites or online applications;

(III) advertisements based on the context of a consumer's current search query, visit to a website, or online application; or page 8-senate bill 21-190

(IV) processing personal data solely for measuring or reporting advertising performance, reach, or frequency.

(26) "Third Party" means a person, public authority, agency, or body other than a consumer, controller, processor, or affiliate of the processor or the controller.

6-1-1304. Applicability of part.

(1) except as specified in subsection (2) of this section, this part 13 applies to a controller that:

(a) conducts business in Colorado or produces or delivers commercial products or services that are intentionally targeted to residents of Colorado; and

(b) satisfies one or both of the following thresholds:

(I) controls or processes the personal data of one hundred thousand consumers or more during a calendar year; or (ii) derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of twenty-five thousand consumers or more.

(II) this Part 13 does not apply to:

(a) protected health information that is collected, stored, and processed by a covered entity or its business associates;

(b) health-care information that is governed by part 8 of article 1 of title 25 solely for the purpose of access to medical records;

(c) patient identifying information, as defined in 42 CFR 2.11, that are governed by and collected and processed pursuant to 42 CFR 2, established pursuant to 42 U.S.C. SEC. 290dd-2;

(d) identifiable private information, as defined in 45 CFR 46.102, for purposes of the federal policy for the protection of human subjects pursuant to 45 CFR 46; identifiable private information that is collected as part of human subjects research pursuant to the ich e6 good clinical practice guideline issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use or the protection of human subjects under 21 CFR 50 and 56; or personal data used or shared in research conducted in accordance with one or more of the categories set forth in this subsection (2)(d);

(e) information and documents created by a covered entity for purposes of complying with HIPAA and its implementing Regulations;

(f) patient safety work product, as defined in 42 CFR 3.20, that is created for purposes of patient safety improvement pursuant to 42 CFR 3, established pursuant to 42 U.S.C. SECS. 299b-21 to 299b-26;

(g) information that is:

(I) de-identified in accordance with the requirements for de-identification set forth in 45 CFR 164; and

(II) derived from any of the health-care-related information described in this section.

(h) information maintained in the same manner as information under subsections (2)(a) to (2)(g) of this section by:

(I) a covered entity or business associate;

(II) a health-care facility or health-care provider; or

(III) a program of a qualified service organization as defined in 42 CFR 2.11;

(i) (i) except as provided in subsection (2)(i)(ii) of this section, an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal data bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by:

(A) a consumer reporting agency as defined in 15 U.S.C. SEC. 1681a (f);

(B) a furnisher of information as set forth in 15 U.S.C. SEC. 1681s-2 that provides information for use in a consumer report, as defined in 15 U.S.C. SEC. 1681a (d); or

(C) a user of a consumer report as set forth in 15 U.S.C. SEC. 1681b.

(II) this subsection (2)(i) applies only to the extent that the activity is regulated by the federal "Fair Credit Reporting Act", 15 U.S.C. SEC. 1681 et seq., as amended, and the personal data are not collected, maintained, disclosed, sold, communicated, or used except as authorized by the federal "Fair Credit Reporting Act", as amended.

(j) personal data:

(I) collected and maintained for purposes of Article 22 of Title 10;

(II) collected, processed, sold, or disclosed pursuant to the federal "Gramm-Leach-Bliley Act", 15 U.S.C. SEC. 6801 et seq., as amended, and implementing regulations, if the collection, processing, sale, or disclosure is in compliance with that law;

(III) collected, processed, sold, or disclosed pursuant to the federal "Driver's Privacy Protection Act of 1994", 18 U.S.C. SEC. 2721 et seq., as amended, if the collection, processing, sale, or disclosure is regulated by that law, including implementing rules, regulations, or exemptions;

(IV) regulated by the federal "Children's Online Privacy Protection Act of 1998", 15 U.S.C. SECS. 6501to 6506, as amended, if collected, processed, and maintained in compliance with that law; or

(V) regulated by the federal "Family Educational Rights and Privacy Act of 1974", 20 U.S.C. SEC. 1232g et seq., as amended, and its implementing regulations;

(k) data maintained for employment records purposes;

(l) an air carrier as defined in and regulated under 49 U.S.C. SEC. 40101 et seq., as amended, and 49 U.S.C. SEC. 41713, as amended;

(m) a national securities association registered pursuant to the federal "Securities Exchange Act of 1934", 15 U.S.C. SEC. 78o-3, as amended, or implementing regulations;

(n) customer data maintained by a public utility as defined in section 40-1-103 (1)(a)(i) or an authority as defined in section 43-4-503 (1), if the data are not collected, maintained, disclosed, sold, communicated, or used except as authorized by state and federal law;

(o) data maintained by a state institution of higher education, as defined in section 23-18-102 (10), the state, the judicial department of the state, or a county, city and county, or municipality if the data is collected, maintained, disclosed, communicated, and used as authorized by state and federal law for noncommercial purposes. this subsection (2)(o) does not effect any other exemption available under this part 13.

(p) information used and disclosed in compliance with 45 CFR 164.512; or

(q) a financial institution or an affiliate of a financial institution as defined by and that is subject to the federal "Gramm-Leach-Bliley Act", 15 U.S.C. SEC. 6801 et seq., as amended, and implementing regulations, including regulation p, 12 CFR 1016.

(3) the obligations imposed on controllers or processors under this part 13 do not:

(a) restrict a controller's or processor's ability to:

(I) comply with federal, state, or local laws, rules, or regulations;

(II) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

(III) cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local law;

(IV) investigate, exercise, prepare for, or defend actual or anticipated legal claims;

(V) conduct internal research to improve, repair, or develop products, services, or technology;

(VI) identify and repair technical errors that impair existing or intended functionality;

(VII) perform internal operations that are reasonably aligned with the expectations of the consumer based on the consumer's existing relationship with the controller;

(VIII) provide a product or service specifically requested by a consumer or the parent or guardian of a child, perform a contract to which the consumer is a party, or take steps at the request of the consumer prior to entering into a contract;

(IX) protect the vital interests of the consumer or of another individual;

(X) prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, or malicious, deceptive, or illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action;

(XI) process personal data for reasons of public interest in the area of public health, but solely to the extent that the processing:

(A) is subject to suitable and specific measures to safeguard the rights of the consumer whose personal data are processed; and

(B) is under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law; or

(XII) assist another person with any of the activities set forth in this subsection (3);

(b) apply where compliance by the controller or processor with this part 13 would violate an evidentiary privilege under Colorado law;

(c) prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under Colorado law as part of a privileged communication;

(d) apply to information made available by a third party that the controller has a reasonable basis to believe is protected speech pursuant to applicable law; and

(e) apply to the processing of personal data by an individual in the course of a purely personal or household activity.

(4) personal data that are processed by a controller pursuant to an exception provided by this section:

(a) shall not be processed for any purpose other than a purpose expressly listed in this section or as otherwise authorized by this part 13; and

(b) shall be processed solely to the extent that the processing is necessary, reasonable, and proportionate to the specific purpose or purposes listed in this section or as otherwise authorized by this Part 13.

(5) if a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that the processing qualifies for the exemption and complies with the requirements in subsection (4) of this section.

6-1-1305. Responsibility according to role.

(1) controllers and processors shall meet their respective obligations established under this part 13.

(2) processors shall adhere to the instructions of the controller and assist the controller to meet its obligations under this part 13. taking into account the nature of processing and the information available to the processor, the processor shall assist the controller by:

(a) taking appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligation to respond to consumer requests to exercise their rights pursuant to section 6-1-1306;

(b) helping to meet the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of the security of the system pursuant to section 6-1-716; and

(c) providing information to the controller necessary to enable the controller to conduct and document any data protection assessments required by section 6-1-1309. The controller and processor are each responsible for only the measures allocated to them.

(3) notwithstanding the instructions of the controller, a processor shall:

(a) ensure that each person processing the personal data is subject to a duty of confidentiality with respect to the data; and

(b) engage a subcontractor only after providing the controller with an opportunity to object and pursuant to a written contract in accordance with subsection (5) of this section that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

(4) taking into account the context of processing, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and establish a clear allocation of the responsibilities between them to implement the measures.

(5) processing by a processor must be governed by a contract between the controller and the processor that is binding on both parties and that sets out:

(a) the processing instructions to which the processor is bound, including the nature and purpose of the processing;

(b) the type of personal data subject to the processing, and the duration of the processing;

(c) the requirements imposed by this subsection (5) and subsections (3) and (4) of this section; and

(d) the following requirements:

(I) at the choice of the controller, the processor shall delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

(II) (A) the processor shall make available to the controller all information necessary to demonstrate compliance with the obligations in this part 13; and

(B) the processor shall allow for, and contribute to, reasonable audits and inspections by the controller or the controller's designated auditor. alternatively, the processor may, with the controller's consent, arrange for a qualified and independent auditor to conduct, at least annually and at the processor's expense, an audit of the processor's policies and technical and organizational measures ii\i support of the obligations under this Part 13 using an appropriate and accepted control standard or framework and audit procedure for the audits as applicable. the processor shall provide a report of the audit to the controller upon request.

(6) in no event may a contract relieve a controller or a processor from the liabilities imposed on them by virtue of its role in the processing relationship as defined by this Part 13.

(7) determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data are to be processed. a person that is not limited in its processing of personal data pursuant to a controller's instructions, or that fails to adhere to the instructions, is a controller and not a processor with respect to a specific processing of data. a processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. if a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, it is a controller with respect to the processing.

(8) (a) a controller or processor that discloses personal data to another controller or processor in compliance with this Part 13 does not violate this Part 13 if the recipient processes the personal data in violation of this Part 13, and, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation.

(b) a controller or processor receiving personal data from a controller or processor in compliance with this Part 13 as specified in subsection (8)(a) of this section does not violate this Part 13 if the controller or processor from which it receives the personal data fails to comply with applicable obligations under this Part 13.

6-1-1306. Consumer personal data rights - repeal.

(1) consumers may exercise the following rights by submitting a request using the methods specified by the controller in the privacy notice required under section 6-1-1308 (1)(a). The method must take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication relating to the request, and the ability of the controller to authenticate the identity of the consumer making the request. Controllers shall not require a consumer to create a new account in order to exercise consumer rights pursuant to this section but may require a consumer to use an existing account. a consumer may submit a request at any time to a controller specifying which of the following rights the consumer wishes to exercise:

(a) Right to opt out.

(I) a consumer has the right to opt out of the processing of personal data concerning the consumer for purposes of:

(A) targeted advertising;

(B) the sale of personal data; or

(C) profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.

(II) a consumer may authorize another person, acting on the consumer's behalf, to opt out of the processing of the consumer's personal data for one or more of the purposes specified in subsection (1)(a)(i) of this section, including through a technology indicating the consumer's intent to opt out such as a web link indicating a preference or browser setting, browser extension, or global device setting. a controller shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf if the controller is able to authenticate, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf.

(III) a controller that processes personal data for purposes of targeted advertising or the sale of personal data shall provide a clear and conspicuous method to exercise the right to opt out of the processing of personal data concerning the consumer pursuant to subsection (1)(a)(i) of this section. The controller shall provide the opt-out method clearly and conspicuously in any privacy notice required to be provided to consumers under this Part 13, and in a clear, conspicuous, and readily accessible location outside the privacy notice.

(IV) (A) a controller that processes personal data for purposes of targeted advertising or the sale of personal data may allow consumers to exercise the right to opt out of the processing of personal data concerning the consumer for purposes of targeted advertising or the sale of personal data pursuant to subsections (1)(a)(i)(a) and (1)(a)(i)(b) of this section by controllers through a user-selected universal opt-out mechanism that meets the technical specifications established by the attorney general pursuant to section 6-1-1313. This subsection (1)(a)(iv)(a) is repealed, effective July 1, 2024.

(B) effective July 1, 2024, a controller that processes personal data for purposes of targeted advertising or the sale of personal data shall allow consumers to exercise the right to opt out of the processing of personal data concerning the consumer for purposes of targeted advertising or the sale of personal data pursuant to subsections (1)(a)(i)(a) and (1)(a)(i)(b) of this section by controllers through a user-selected universal opt-out mechanism that meets the technical specifications established by the attorney general pursuant to section 6-1-1313.

(C) notwithstanding a consumer's decision to exercise the right to opt out of the processing of personal data through a universal opt-out mechanism pursuant to subsection (1)(a)(iv)(b) of this section, a controller may enable the consumer to consent, through a web page, application, or a similar method, to the processing of the consumer's personal data for purposes of targeted advertising or the sale of personal data, and the consent takes precedence over any choice reflected through the universal opt-out mechanism. before obtaining a consumer's consent to process personal data for purposes of targeted advertising or the sale of personal data pursuant to this subsection (1)(a)(iv)(c), a controller shall provide the consumer with a clear and conspicuous notice informing the consumer about the choices available under this section, describing the categories of personal data to be processed and the purposes for which they will be processed, and explaining how and where the consumer may withdraw consent. the web page, application, or other means by which a controller obtains a consumer's consent to process personal data for purposes of targeted advertising or the sale of personal data must also allow the consumer to revoke the consent as easily as it is affirmatively provided.

(b) **Right of access.** A consumer has the right to confirm whether a controller is processing personal data concerning the consumer and to access the consumer's personal data.

(c) **Right to correction.** A consumer has the right to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.

(d) **Right to deletion**. A consumer has the right to delete personal data concerning the consumer.

(e) **Right to data portability.** When exercising the right to access personal data pursuant to subsection (1)(b) of this section, a consumer has the right to obtain the personal data in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another entity without hindrance. A consumer may exercise this right no more than two times per calendar year. Nothing in this subsection (1)(e) requires a controller to provide the data to the consumer in a manner that would disclose the controller's trade secrets.

(2) **Responding to consumer requests.** (a) a controller shall inform a consumer of any action taken on a request under subsection (1) of this section without undue delay and, in any event, within forty-five days after receipt of the request. the controller may extend the forty-five-day period by forty-five additional days where reasonably necessary, taking into account the complexity and number of the requests. the controller shall inform the consumer of an extension within forty-five days after receipt of the request, together with the reasons for the delay.

(b) If a controller does not take action on the request of a consumer, the controller shall inform the consumer, without undue delay and, at the latest, within forty-five days after receipt of the request, of the reasons for not taking action and instructions for how to appeal the decision with the controller as described in subsection (3) of this section.

(c) Upon request, a controller shall provide to the consumer the information specified in this section free of charge; except that, for a second or subsequent request within a twelve-month period, the controller may charge an amount calculated in the manner specified in section 24-72-205 (5)(a).

(d) A controller is not required to comply with a request to exercise any of the rights under subsection (1) of this section if the controller is unable to authenticate the request using commercially reasonable efforts, in which case the controller may request the provision of additional information reasonably necessary to authenticate the request.

(3) (a) a controller shall establish an internal process whereby consumers may appeal a refusal to take action on a request to exercise any of the rights under subsection (1) of this section within a reasonable period after the consumer's receipt of the notice sent by the controller under subsection (2)(b) of this section. the appeal process must be conspicuously available and as easy to use as the process for submitting a request under this section.

(b) within forty-five days after receipt of an appeal, a controller shall inform the consumer of any action taken or not taken in response to the appeal, along with a written explanation of the reasons in support of the response. The controller may extend the forty-five-day period by sixty additional days where reasonably necessary, taking into account the complexity and number of requests serving as the basis for the appeal. The controller shall inform the consumer of an extension within forty-five days after receipt of the appeal, together with the reasons for the delay.

(c) the controller shall inform the consumer of the consumer's ability to contact the attorney general if the consumer has concerns about the result of the appeal.

6-1-1307. Processing de-identified data.

(1) this part 13 does not require a controller or processor to do any of the following solely for purposes of complying with this part 13:

(a) reidentify de-identified data;

(b) comply with an authenticated consumer request to access, correct, delete, or provide personal data in a portable format pursuant to section 6-1-1306 (1), if all of the following are true:

(I) (A) the controller is not reasonably capable of associating the request with the personal data; or (b) it would be unreasonably burdensome for the controller to associate the request with the personal data;

(II) the controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data or associate the personal data with other personal data about the same specific consumer; and

(III) the controller does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party, except as otherwise authorized by the consumer; or

(c) maintain data in identifiable form or collect, obtain, retain, or access any data or technology in order to enable the controller to associate an authenticated consumer request with personal data.

(2) a controller that uses de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the de-identified data are subject and shall take appropriate steps to address any breaches of contractual commitments.

(3) the rights contained in section 6-1-1306 (1)(b) to (1)(e) do not apply to pseudonymous data if the controller can demonstrate that the information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

6-1-1308. Duties of controllers.

(1) **Duty of transparency.** (a) a controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

(I) the categories of personal data collected or processed by the controller or a processor;

(II) the purposes for which the categories of personal data are processed;

(III) how and where consumers may exercise the rights pursuant to section 6-1-1306, including the controller's contact information and how a consumer may appeal a controller's action with regard to the consumer's request;

(IV) the categories of personal data that the controller shares with third parties, if any; and

(V) the categories of third parties, if any, with whom the controller shares personal data.

(b) if a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose the sale or processing, as well as the manner in which a consumer may exercise the right to opt out of the sale or processing.

(c) a controller shall not:

(I) require a consumer to create a new account in order to exercise a right; or

(II) based solely on the exercise of a right and unrelated to feasibility or the value of a service, increase the cost of, or decrease the availability of, the product or service.

(d) nothing in this Part 13 shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discount, or club card program.

(2) **Duty of purpose specification.** a controller shall specify the express purposes for which personal data are collected and processed.

(3) **Duty of data minimization.** A controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes for which the data are processed.

(4) **Duty to avoid secondary use.** A controller shall not process personal data for purposes that are not reasonably necessary to or compatible with the specified purposes for which the personal data are processed, unless the controller first obtains the consumer's consent.

(5) **Duty of care.** A controller shall take reasonable measures to secure personal data during both storage and use from unauthorized acquisition. The data security practices must be appropriate to the volume, scope, and nature of the personal data processed and the nature of the business.

(6) **Duty to avoid unlawful discrimination.** A controller shall not process personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers.

(7) **Duty regarding sensitive data.** A controller shall not process a consumer's sensitive data without first obtaining the consumer's consent or, in the case of the processing of personal data concerning a known child, without first obtaining consent from the child's parent or lawful guardian.

6-1-1309. Data protection assessments - attorney general access and evaluation - definition.

(1) a controller shall not conduct processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment of each of its processing activities that involve personal data acquired on or after the effective date of this section that present a heightened risk of harm to a consumer.

(2) for purposes of this section, "processing that presents a heightened risk of harm to a consumer" includes the following:

(a) processing personal data for purposes of targeted advertising or for profiling if the profiling presents a reasonably foreseeable risk of:

(I) unfair or deceptive treatment of, or unlawful disparate impact on, consumers;

(II) financial or physical injury to consumers;

(III) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person; or

(IV) other substantial injury to consumers;

(b) selling personal data; and

(c) processing sensitive data.

(3) Data protection assessments must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards that the controller can employ to reduce the risks. The controller shall factor into this assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

(4) A controller shall make the data protection assessment available to the attorney general upon request. The attorney general may evaluate the data protection assessment for compliance with the duties contained in section 6-1-1308 and with other laws, including this article 1. Data protection assessments are confidential and exempt from public inspection and copying under the "Colorado Open Records Act", part 2 of article 72 of title 24. The disclosure of a data protection assessment pursuant to a request from the attorney general under this subsection (4) does not constitute a waiver of any attorney-client privilege or work-product protection that might otherwise exist with respect to the assessment and any information contained in the assessment.

(5) A single data protection assessment may address a comparable set of processing operations that include similar activities.

(6) Data protection assessment requirements apply to processing activities created or generated after July 1, 2023, and are not retroactive.

6-1-1310. Liability.

(1) Notwithstanding any provision in part 1 of this article 1, this Part 13 does not authorize a private right of action for a violation of this part 13 or any other provision of law. This subsection (1) neither relieves any party from any duties or obligations imposed, nor alters any independent rights that consumers have, under other laws, including this Article 1, the state constitution, or the united states constitution.

(2) Where more than one controller or processor, or both a controller and a processor, involved in the same processing violates this Part 13, the liability shall be allocated among the parties according to principles of comparative fault.

6-1-1311. Enforcement - penalties - repeal.

(1) (a) Notwithstanding any other provision of this article 1, the attorney general and district attorneys have exclusive authority to enforce this Part 13 by bringing an action in the name of the state or as parens patriae on behalf of persons residing in the state to enforce this Part 13 as provided in this Article 1, including seeking an injunction to enjoin a violation of this Part 13.

(b) Notwithstanding any other provision of this article 1, nothing in this Part 13 shall be construed as providing the basis for, or being subject to, a private right of action for violations of this Part 13 or any other law.

(c) For purposes only of enforcement of this part 13 by the attorney general or a district attorney, a violation of this part 13 is a deceptive trade practice.

(d) Prior to any enforcement action pursuant to subsection (1)(a) of this section, the attorney general or district attorney must issue a notice of violation to the controller if a cure is deemed possible. if the controller fails to cure the violation within sixty days after receipt of the notice of violation, an action may be brought pursuant to this section. this subsection (1)(d) is repealed, effective January 1, 2025.

(2) The state treasurer shall credit all receipts from the imposition of civil penalties under this Part 13 pursuant to section 24-31-108.

6-1-1312. Preemption - local governments.

This Part 13 supersedes and preempts laws, ordinances, resolutions, regulations, or the equivalent adopted by any statutory or home rule municipality, county, or city and county regarding the processing of personal data by controllers or processors.

6-1-1313. Rules - opt-out mechanism.

(1) The attorney general may promulgate rules for the purpose of carrying out this Part 13.

(2) By July 1, 2023, the attorney general shall adopt rules that detail the technical specifications for one or more universal opt-out mechanisms that clearly communicate a consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of personal data for purposes of targeted advertising or the sale of personal data pursuant to section 6-1-1306 (1)(a)(i)(a) or (1)(a)(i)(b). The attorney general may update the rules that detail the technical specifications for the mechanisms from time to time to reflect the means by which consumers interact with controllers. The rules must:

(a) not permit the manufacturer of a platform, browser, device, or any other product offering a universal opt-out mechanism to unfairly disadvantage another controller;

(b) require controllers to inform consumers about the opt-out choices available under section 6-1-1306 (1)(a)(i);

(c) not adopt a mechanism that is a default setting, but rather clearly represents the consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of personal data pursuant to section 6-1-1306 (1)(a)(i)(a) or (1)(a)(i)(b);

(d) adopt a mechanism that is consumer-friendly, clearly described, and easy to use by the average consumer;

(e) adopt a mechanism that is as consistent as possible with any other similar mechanism required by law or regulation in the united states; and

(f) permit the controller to accurately authenticate the consumer as a resident of this state and determine that the mechanism represents a legitimate request to opt out of the processing of personal data for purposes of targeted advertising or the sale of personal data pursuant to section 6-1-1306 (1)(a)(i)(a) or (1)(a)(i)(b).

(3) By January 1, 2025, the attorney general may adopt rules that govern the process of issuing opinion letters and interpretive guidance to develop an operational framework for business that includes a good faith reliance defense of an action that may otherwise constitute a violation of this part 13. The rules must become effective by July 1, 2025.

Colorado Privacy Act Rules

PART 1 GENERAL APPLICABILITY

Rule 1.01 BASIS, SPECIFIC STATUTORY AUTHORITY, AND PURPOSE

The rules in this Part 904-3 are developed pursuant to C.R.S. § 6-1-108(1), which grants the Attorney General the authority to promulgate such rules as may be necessary to administer the provisions of the Colorado Consumer Protection Act, and to C.R.S. § 6-1-1313, which gives the Attorney General authority to promulgate Rules for the purpose of carrying out the Colorado Privacy Act and requires the Attorney General to adopt Rules that detail the technical specifications for one or more Universal Opt-Out Mechanisms that clearly communicate a Consumer's affirmative, freely given, and unambiguous choice to opt out of the Processing of Personal Data for purposes of Targeted Advertising or the Sale of Personal Data pursuant to C.R.S. §§ 6-1-1306(1)(a)(I)(A) or (1)(a)(I)(B).

These rules are promulgated to establish implementation and operational guidelines for the Colorado Privacy Act, and to help ensure that the Colorado Privacy Act is carried out in a way that is consistent with the intent of the General Assembly, as reflected in the legislative declaration at C.R.S. § 6-1-1302.

PART 2 DEFINITIONS

Rule 2.01 AUTHORITY AND PURPOSE

A. The statutory authority for the rules in this Part 2 is C.R.S. §§ 6-1-108(1), 6-1-1303, and 6-1- 1313. The purpose of these rules is to define certain undefined terms that are used throughout the Colorado Privacy Act, C.R.S. § 6-1-1301, *et seq*., and these Colorado Privacy Act Rules, 4 CCR 904-3, including but not limited to certain undefined terms that are used in the definitions set forth in C.R.S. § 6-1-1303. The terms defined by this rule and C.R.S. § 6-1-1303 are capitalized where they appear in the rules to let the reader know to refer back to the definitions. When a term is used in a conventional sense, and is not intended to be a defined term, it is not capitalized.

Rule 2.02 DEFINED TERMS

The following definitions of terms, in addition to those set forth in C.R.S. § 6-1-1303, apply to these Colorado Privacy Act Rules, 4 CCR 904-3, promulgated pursuant to the Colorado Privacy Act, unless the context requires otherwise:

"**Authorized Agent**" as referred to in C.R.S. § 6-1-1306(1)(a)(II) means a person or entity authorized by the Consumer to act on the Consumer's behalf.

"**Biometric Data**" as referred to in C.R.S. § 6-1-1303(24)(b) means Biometric Identifiers that are used or intended to be used, singly or in combination with each other or with other Personal Data, for identification purposes. Unless such data is used for identification purposes, "Biometric Data" does not include (a) a digital or physical photograph, (b) an audio or voice recording, or (c) any data generated from a digital or physical photograph or an audio or video recording.

"**Biometric Identifiers**" means data generated by the technological processing, measurement, or analysis of an individual's biological, physical, or behavioral characteristics that can be Processed for the purpose of uniquely identifying an individual, including but not limited to a fingerprint, a voiceprint, scans or records of eye retinas or irises, facial mapping, facial geometry, facial templates, or other unique biological, physical, or behavioral patterns or characteristics.

"**Bona Fide Loyalty Program**" as referred to in C.R.S. § 1-6-1308(1)(d) is defined as a loyalty, rewards, premium feature, discount, or club card program established for the genuine purpose of providing Bona Fide Loyalty Program Benefits to Consumers that voluntarily participate in that program, such that the primary purpose of Processing Personal Data through the program is solely to provide Bona Fide Loyalty Program Benefits to participating Consumers.

"**Bona Fide Loyalty Program Benefit**" is defined as an offer of superior price, rate, level, quality, or selection of goods or services provided to a Consumer through a Bona Fide Loyalty Program. Such benefits may be provided directly by a Controller or through a Bona Fide Loyalty Program Partner.

"**Bona Fide Loyalty Program Partner**" is defined as a Third Party that provides Bona Fide Loyalty Program Benefits to Consumers through a Controller's Bona Fide Loyalty Program, either alone or in partnership with the Controller.

"**Commercial product or service**" as referred to in C.R.S. § 6-1-1304(1)(a) means a product or service bought, sold, leased, joined, provided, subscribed to, or delivered in exchange for monetary or other valuable consideration in the course of a Controller's business, vocation, or occupation.

"**Controller**" is defined as set forth in C.R.S. § 6-1-1303(7), and means a person that, alone or jointly with others, determines the purposes for and means of Processing Personal Data.

"**Data Broker**" is defined as a Controller that knowingly collects and sells to Third Parties the Personal Data of a Consumer with whom the Controller does not have a direct relationship.

"**Data Right**" or "**Data Rights**" means the Consumer Personal Data rights granted in C.R.S. § 6-1- 1306(1).

"**Disability**" or "**Disabilities**" has the same meaning as set forth in C.R.S. § 24-85-102(2.3).

"**Employee**" means any person, acting as a job applicant to, or performing labor or services for the benefit of an Employer, including contingent and temporary workers and migratory laborers.

"**Employer**" means every person, entity, firm, partnership, association, corporation, migratory field labor contractor or crew leader, receiver, or other officer of court, and any agent or officer thereof, of the above- mentioned classes, employing any person.

"**Employment Records**" as referred to in C.R.S. § 6-1-1304(2)(k) means the records of an Employee, maintained by the Employer in the context of the Employer-Employee relationship having to do with hiring, promotion, demotion, transfer, lay-off or termination, rates of pay or other terms of compensation, as well as other information maintained because of the Employer-Employee relationship.

"**Human Involved Automated Processing**" means the automated processing of Personal Data where a human (1) engages in a meaningful consideration of available data used in the Processing or any output of the Processing and (2) has the authority to change or influence the outcome of the Processing.

"**Human Reviewed Automated Processing**" means the automated processing of Personal Data where a human reviews the automated processing, but the level of human engagement does not rise to the level required for Human Involved Automated Processing. Reviewing the output of the automated processing with no meaningful consideration does not rise to the level of Human Involved Automated Processing.

"**Information that a Controller has a reasonable basis to believe the Consumer has lawfully made available to the general public**" as referred to in C.R.S. § 6-1-1303(17)(b) means information that a Consumer has intentionally made available to the general public or information that a Consumer has made available under federal or state law, which may include but is not limited to:

1. Personal Data found in a telephone book, a television or radio program, or a national or local news publication;

2. Personal Data that has been intentionally made available by the Consumer through a website or online service where the Consumer has not restricted the information to a specific audience;

3. A visual observation of an individual's physical presence in a public place by another person, not including data collected by a device in the individual's possession; and

4. A disclosure that has been made to the general public as required by federal, state, or local law.

"**Intimate Image**" means any visual depiction, photograph, film, video, recording, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, that depicts an identified or identifiable person's private parts, or a person engaged in a private act, in circumstances in which a reasonable person would reasonably expect to be afforded privacy.

"**Noncommercial Purpose**" as referred to in C.R.S. § 6-1-1304(2)(o) includes, but is not limited to, the following activities when conducted by: (a) a state institution of higher education, as defined in C.R.S. § 23-18-102(10), the state, the judicial department of the state, or a county, city and county, or municipality; or (b) a Processor acting on behalf of one or more of the foregoing:

1. Processing activities related to the delivery of services and benefits;

2. Research purposes;

3. Budgeting;

4. Improving operations or the delivery services or benefits;

5. Auditing operations or service or benefit delivery;

6. Sharing Personal Data between these categories of entities for any of these purposes; or

7. Any other purpose related to speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.

"**Opt-Out Purpose**" or "**Opt-Out Purposes**" means the categories of Personal Data Processing from which the Consumer may opt out pursuant to C.R.S. § 6-1-1306(1)(a).

"**Personal Data**" is defined as set forth in C.R.S. § 6-1-1303(17), and (a) means information that is linked or reasonably linkable to an identified or identifiable individual; and (b) does not include de-identified data or Publicly Available Information as used in (17)(b).

"**Process**" or "**Processing**" is defined as set forth in C.R.S. § 6-1-1303(18), and means the collection, use, sale, storage, disclosure, analysis, deletion, or modification of Personal Data and includes the actions of a Controller directing a Processor to Process Personal Data.

"**Processor**" is defined as set forth in C.R.S. § 6-1-1303(19), and means a person that Processes Personal Data on behalf of a Controller.

"**Profiling**" is defined as set forth in C.R.S. § 6-1-1303(20), and means any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

"**Publicly Available Information**" is defined as set forth in C.R.S. § 6-1-1303(17), and does not include:

1. Any Personal Data obtained or processed in in violation of C.R.S. §§ 18-7-107 or 18-7- 801;

2. Biometric Data;

3. Genetic Information; or

4. Nonconsensual Intimate Images known to the Controller.

"**Revealing**" as referred to in C.R.S. § 6-1-1303(24)(a) includes Sensitive Data Inferences. For example:

1. While precise geolocation information at a high level may not be considered Sensitive Data, precise geolocation data which is used to infer an individual visited a mosque and is used to infer that individual's religious beliefs is considered Sensitive Data under C.R.S. § 6-1-1303(24)(a). Similarly, precise geolocation data which is used to infer an individual visited a reproductive health clinic and is used to infer an individual's health condition or sex life is considered Sensitive Data under C.R.S. § 6-1-1303(24)(a).

2. While web browsing data at a high level may not be considered Sensitive Data, web browsing data which, alone or in combination with other Personal Data, infers an individual's sexual orientation is considered Sensitive Data under C.R.S. § 6-1- 1303(24)(a).

"**Sensitive Data Inference**" or "**Sensitive Data Inferences**" means inferences made by a Controller based on Personal Data, alone or in combination with other data, which are used to indicate an individual's racial or ethnic origin; religious beliefs; mental or physical health condition or diagnosis; sex life or sexual orientation; or citizenship or citizenship status.

"**Solely Automated Processing**" means the automated processing of Personal Data with no human review, oversight, involvement, or intervention.

"**Universal Opt-Out Mechanism**" or "**Universal Opt-Out Mechanisms**" means mechanisms that clearly communicate a Consumer's affirmative, freely given, and unambiguous choice to opt out of the Processing of Personal Data for purposes of Targeted Advertising or the Sale of Personal Data pursuant to C.R.S. § 6-1-1306 (1)(a)(I)(A) or (1)(a)(I)(B), which meets the technical specifications set forth in 4 CCR 904-3, Rule 5.06 pursuant to C.R.S. § 6-1-1313(2).

PART 3 CONSUMER DISCLOSURES

Rule 3.02 REQUIREMENTS FOR DISCLOSURES, NOTIFICATIONS, AND OTHER COMMUNICATIONS TO CONSUMERS

A. Disclosures, notifications, and other communications to Consumers pursuant to 4 CCR 904-3, Rules 4.02, 4.05(D), 5.03, 6.02, 6.05, and 7.04 must be:

1. Designed to be understandable and accessible to a Controller's target audiences, considering the vulnerabilities or unique characteristics of the audience and paying particular attention to the vulnerabilities of children. For example, they shall use plain, straightforward language and avoid technical or legal jargon.

2. Reasonably accessible to Consumers with Disabilities, including through the use of digital accessibility tools. For notices provided online, the Controller shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference as described at 4 CCR 904-3, Rule 11.02. In other contexts, the Controller shall provide information on how a Consumer with a Disability may access the disclosure or communication or make a request in an alternative format.

3. Available in the languages in which the Controller in its ordinary course provides web pages, interfaces, contracts, disclaimers, sale announcements, and other information to Consumers. Disclosures and communications sent directly to Consumers must be sent in the language in which the Consumer ordinarily interacts with the Controller.

4. Available through a readily accessible interface regularly used in conjunction with the Controller's product or service.

5. Provided in a readable format on all devices through which Consumers normally or regularly interact with the Controller, including on smaller screens and through mobile applications, if applicable.

6. Unless otherwise stated, communicated in a manner by which the Controller regularly interacts with Consumers.

7. Straightforward and accurate, and must not be written or presented in a way that is unfair, deceptive, false, or misleading.

PART 4 CONSUMER PERSONAL DATA RIGHTS

Rule 4.02 SUBMITTING REQUESTS TO EXERCISE PERSONAL DATA RIGHTS

A. Pursuant to C.R.S. § 6-1-1306(1), a Controller's privacy notice must include specific methods through which a Consumer may submit requests to exercise Data Rights.

B. Any method specified by a Controller pursuant to this rule must comply with each of the following:

1. Consider the ways in which Consumers normally interact with the Controller:

   a. A Controller that interacts with Consumers exclusively online and has a direct relationship with a Consumer from whom it collects Personal Data shall only be required to provide an email address for submitting access, correction, deletion, or data portability requests.

   b. A Controller that does not fall within subsection 4 CCR 904-3, Rule 4.02(B)(1)(a) shall provide two or more designated methods for submitting a Data Rights request. If a Controller maintains a website, mobile application, or other digital presence, one method for submitting requests shall be through its website, mobile application, or digital interface, such as through a webform;

   c. If a Controller interacts with Consumers in person, the Controller shall consider providing an in-person method such as a printed form the Consumer can directly submit or send by mail; a tablet or computer portal that allows the Consumer to complete and submit an online form; or a telephone by which the Consumer can call the Controller's toll-free number.

2. Enable the Consumer to submit the request to the Controller at any time;

3. Comply with requirements for disclosures, notifications, and other communications to Consumers provided in 4 CCR 904-3, Rule 3.02;

4. Use reasonable data security measures, consistent with 4 CCR 904-3, Rule 6.09, when exchanging information in furtherance of Data Rights requests, considering the volume, scope and nature of Personal Data that may be exchanged; and

5. Be easy for Consumers to execute, requiring a minimal number of steps.

C. The Data Rights request method does not have to be specific to Colorado, so long as the request method:

1. Clearly indicates which rights are available to Colorado Consumers;

2. Provides all Data Rights available to Colorado Consumers;

3. Provides Colorado Consumers a clear understanding of how to exercise their rights; and

4. Meets all other requirements of this part, 4 CCR 904-3, Rule 4.02.

D. When a Consumer submits a Data Rights request, a Controller may only collect Personal Data through the request process if the Personal Data is reasonably necessary to Authenticate the Consumer, respond to the request, or effectuate the Data Rights request.

E. A Controller must not require a Consumer to create a new user account to exercise their Data Rights request, but may require a Consumer to use an existing password-protected account.

Rule 4.03 RIGHT TO OPT OUT

A. A Controller shall comply with an opt-out request by:

1. Ceasing to Process the Consumer's Personal Data for the Opt-Out Purpose(s) as soon as feasibly possible and without undue delay from the date the Controller receives the request, taking into account the size and complexity of the Controller's businesses and burden of operationalizing the opt-out.

   a. If a Controller does not know the identity of a Consumer submitting an online opt- out request, such that the Controller is unable to opt the Consumer out of the Processing of offline or other connected Personal Data, the Controller may request the additional information necessary to do so subject to 4 CCR 904-3, Rules 4.08 and 5.05.

   b. If a Consumer submits a request to exercise more than one Data Right and a Controller is able to complete the opt-out request in a more timely manner than other Data Rights requests, the Controller should complete the opt-out request prior to any other Data Rights request.

2. Maintaining a record of the opt-out request and response, in compliance with 4 CCR 904- 3, Rule 6.11.

3. Using agreed upon technical, organizational or other measures or processes to instruct its Processors, pursuant to C.R.S. § 6-1-1305(2)(a), to stop Processing the Personal Data as needed to effectuate the Consumer's opt-out request.

B. To enable a Consumer to exercise the right to opt out of the Opt-Out Purposes provided in C.R.S. § 6-1-1306(1)(a)(I), a Controller must provide the disclosures required by C.R.S. § 6-1- 1308(1)(b).

1. A Controller that Sells Personal Data or Processes Personal Data for Targeted Advertising must also provide a clear and conspicuous method for Consumers to exercise the right to opt out of the Processing of Personal Data for each or all of the Opt- Out Purposes, as applicable.

   a. The clear, conspicuous method must be provided either directly or through a link, in a clear, conspicuous, and readily accessible location outside the privacy notice.

2. A Controller Processing Personal Data for Profiling in furtherance of a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health- care services, or access to essential goods or services, as subject to the opt-out right provided at C.R.S. § 6-1-1306(1)(a)(I), shall provide a clear and conspicuous method for Consumers to exercise the right to opt out of Processing Personal Data for such Profiling at or before the time such Processing occurs.

3. Any clear and conspicuous method for Consumers to exercise the right to opt out of Processing for the Opt-Out Purposes, provided pursuant to this section, must comply with the requirements of 4 CCR 904-3, Rule 4.02(B). If a link is used, it must take a Consumer directly to the opt-out method and the link text must provide a clear understanding of its purpose, for example "Colorado Opt-Out Rights," "Personal Data Use Opt-Out," "Your Opt-Out Rights," "Your Privacy Choices," or "Your Colorado Privacy Choices."

C. An Authorized Agent may exercise a Consumer's opt-out right on behalf of the Consumer, so long as the Controller is able to, with commercially reasonable effort, Authenticate the identity of the Consumer and the Authorized Agent's authority to act on the Consumer's behalf.

D. A Controller may collect the Consumer's Personal Data necessary to effectuate the Consumer's opt-out right, pursuant to 4 CCR 904-3, Rule 4.02(D).

Rule 4.04 RIGHT OF ACCESS

A. A Controller shall comply with an access request by providing the Consumer all the specific pieces of Personal Data it has collected and maintains about the Consumer that are the subject of the request, including without limitation, any Personal Data that the Controller's Processors obtained from the Controller in providing services to the Controller.

1. Specific pieces of Personal Data include final Profiling decisions, inferences, derivative data, marketing profiles, and other Personal Data created by the Controller which is linked or reasonably linkable to an identified or identifiable individual.

B. Personal Data provided in response to an access request must:

1. Be provided in in a form that is concise, transparent and easily intelligible and in an appropriate, commonly used electronic format, depending on the nature of the data;

2. Be available in the language in which the Consumer interacts with the Controller.

3. Avoid incomprehensible internal codes and, if necessary, include explanations that would allow the average Consumer to make an informed decision of whether to exercise deletion, correction, or opt-out rights.

4. Be provided in compliance with the requirements for disclosures, notifications, and other communications, as described in 4 CCR 904-3, Rule 3.02, as applicable.

C. The Controller shall implement and maintain reasonable data security measures, consistent with 4 CCR 904-3, Rule 6.09, in Processing any documentation relating to a Consumer's access request.

D. A Controller shall not be required to disclose in response to an access request a Consumer's government-issued identification number, financial account number, health insurance or medical identification number, an account password, security questions and answers, Biometric Data, or Biometric Identifiers. The Controller shall, however, inform the Consumer with sufficient particularity that it has collected that type of information. For example, a Controller shall respond that it collects "unique Biometric Data including a fingerprint scan" without disclosing the actual fingerprint scan data.

E. If a Consumer exercises the right to access their Personal Data in a portable format pursuant to C.R.S. § 6-1-1306(1)(e) and the Controller determines the manner of response would reveal the Controller's trade secrets, the Controller must still honor the Consumer's undiminished right of access in a format or manner which would not reveal trade secrets, such as in a nonportable format.

Rule 4.05 RIGHT TO CORRECTION

A. Consumers have the right to correct inaccuracies in their Personal Data subject to C.R.S. § 6-1- 1306(c).

B. A Controller shall comply with a Consumer's correction request by correcting the Consumer's Personal Data in its existing systems, except archive or backup systems. The Controller shall also use agreed upon technical, organizational, or other measures or processes to instruct its Processors, pursuant to C.R.S. § 6-1-1305(2)(a), to make the necessary corrections in their respective systems.

C. If a Controller or Processor stores any Personal Data on archived or backup systems, it may delay compliance with the Consumer's correction request with respect to an archived or backup system until that system is restored to an active system or is next accessed or used.

D. If a Consumer submits a request to exercise their right to correct Personal Data and the requested correction to that Personal Data could be made by the Consumer through the Consumer's account settings, a Controller may respond to the Consumer's request by providing instructions on how the Consumer may correct the Personal Data so long as:

1. The correction process is not unduly burdensome to the Consumer;

2. The instructions meet all requirements of 4 CCR 904-3, Rule 3.02;

3. The Controller's response is compliant with the timing requirements set forth in C.R.S. § 6-1-1306(2)(a); and

4. The process described in the instructions enable the Consumer to make the specific requested correction.

E. A Controller may require the Consumer to provide documentation if necessary to determine whether the Personal Data, or the Consumer's requested correction to the Personal Data, is accurate.

1. When requesting documentation, the Controller must provide the Consumer with a meaningful understanding of why the documentation is necessary.

2. Any documentation provided by the Consumer in connection with the Consumer's right to correction shall only be Processed by the Controller in considering the accuracy of the Consumer's Personal Data.

3. The Controller shall implement and maintain reasonable data security measures, consistent with 4 CCR 904-3, Rule 6.09, in Processing any documentation relating to the Consumer's correction request.

4. If the Controller did not receive the Personal Data directly from the Consumer and has no documentation to support the accuracy of the Personal Data, the Consumer's assertion of inaccuracy shall be sufficient to establish that the Personal Data is inaccurate.

5. A Controller, having exhausted the steps above may decide not to act upon a Consumer's correction request if the Controller determines that the contested Personal Data is more likely than not accurate.

   a. If a Controller denies a Consumer's correction request based on the Controller's determination that the contested Personal Data is more likely than not accurate, the Controller must describe in documentation required by 4 CCR 904-3, Rule 6.11(A), the Consumer's requested correction to the Personal Data, any documentation requested from and provided by the Consumer in support of the correction request, and the reason for the Controller's determination that the Consumer's documentation was not sufficient to support the Consumer's position.

Rule 4.06 RIGHT TO DELETION

A. A Controller shall comply with a Consumer's deletion request by:

1. Permanently and completely erasing the Personal Data from its existing systems, except archive or backup systems, or de-identifying the Personal Data such that it cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such an individual, in accordance with C.R.S. § 6-1-1303(11); and

2. Using agreed upon technical, organizational, or other measures, or processes to instruct its Processors pursuant to C.R.S. § 6-1-1305(2)(b) to delete the Consumer's Personal Data held by the Processors.

B. Notwithstanding 4 CCR 904-3, Rule 4.06(A), a Controller may maintain records of a Consumer's deletion request consistent with 4 CCR 904-3, Rule 6.11 and as needed to effectuate the deletion request.

C. If a Controller or Processor stores any Personal Data on archived or backup systems, it may delay compliance with the Consumer's deletion request with respect to an archived or backup system until that system is restored to an active system or is next accessed or used.

D. A Controller that has obtained Personal Data about a Consumer from a source other than the Consumer shall comply with a Consumer's deletion request with respect to that Personal Data pursuant to C.R.S. § 6-1-1306(d) by (i) retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the Consumer's Personal Data remains deleted from the Consumer's records and not using such retained data for any other purpose, or (ii) opting the Consumer out of the Processing of such Personal Data for any purpose except for those exempted pursuant to the provisions of C.R.S. § 6-1-1304.

E. If a Controller complies with a deletion request by opting the Consumer out of Processing under 4.06(D) or does not opt the Consumer out of some Processing of Personal Data because the Processing purpose is exempted pursuant to the provisions of C.R.S. § 6-1-1304, the Controller shall provide the Consumer with the categories of Personal Data that were not deleted along with any applicable exception. The Controller shall not use the Consumer's Personal Data retained for any other purpose than provided for by the applicable exception.

Rule 4.07 RIGHT TO DATA PORTABILITY

A. To comply with a data portability request, a Controller must transfer to a Consumer the Personal Data it has collected and maintains about the Consumer through a secure method in a commonly used electronic format that, to the extent technically feasible, is readily usable and allows the Consumer to transmit the Personal Data to another entity without hindrance.

Pursuant to C.R.S. § 6-1-1306(1)(e), a Controller is not required to provide Personal Data to a Consumer in a manner that would disclose the Controller's trade secrets. When complying with a request to access Personal Data in a portable format, Controllers must provide as much data as possible in a portable format without disclosing the trade secret.

1. For example, if sharing both raw or unedited Personal Data along with related inferences or derived Personal Data in an Excel file would reveal a trade secret, the Controller may provide either set of Personal Data in an Excel file, so long as it is clear to the Consumer that the Controller maintains both types of Personal Data.

Rule 4.08 AUTHENTICATION

A. Pursuant to C.R.S. § 6-1-1306(1), a Controller shall use a commercially reasonable method for authenticating the identity of every Consumer submitting any Data Right request, and the authority of every Authorized Agent submitting an opt-out request on behalf of a Consumer pursuant to C.R.S. § 6-1-1306(1)(a)(II).

1. To determine if an authentication method is commercially reasonable, the Controller shall consider the Data Rights exercised, the type, sensitivity, value, and volume of Personal Data involved, the level of possible harm that improper access or use could cause to the Consumer submitting the Data Right request and the cost of authentication to the Controller. A Controller must avoid methods that place an unreasonable burden on the Consumer submitting a Data Right request, or Authorized Agent submitting an opt-out request on behalf of a Consumer.

B. When possible, a Controller shall avoid requesting additional Personal Data to Authenticate a Consumer unless the Controller cannot Authenticate the Consumer using the Personal Data already maintained by the Controller.

C. Personal Data obtained to Authenticate a Consumer may only be used to Authenticate the Consumer submitting the Data Right request, pursuant to C.R.S. § 6-1-1306(1), or to Authenticate an Authorized Agent's authority, pursuant C.R.S. § 6-1-1306(1)(a)(II), and must be deleted as soon as practical after Processing the Consumer's request, except as required by 4 CCR 904-3, Rule 6.11, or as otherwise required.

D. A Controller shall implement reasonable security measures, consistent with 4 CCR 904-3, Rule 6.09, to protect Personal Data exchanged to Authenticate a Consumer or to Authenticate an Authorized Agent's authority, considering the type, value, sensitivity, and volume of information exchanged and the level of possible harm improper access or use could cause to the Consumer submitting a Data Right request.

E. A Controller shall not require the Consumer or Authorized Agent to pay a fee for authentication. For example, a Controller may not require a Consumer to provide a notarized affidavit for authentication unless the Controller compensates the Consumer for the cost of notarization.

F. If a Controller cannot Authenticate the Consumer submitting a Data Right request using commercially reasonable efforts, the Controller is not required to comply with the Consumer's request. The Controller shall inform the Consumer that their identity could not be authenticated, provide information on how to remedy any deficiencies, and may request additional Personal Data if reasonably necessary to Authenticate the Consumer.

Rule 4.09 RESPONDING TO CONSUMER REQUESTS

A. A Controller must respond to a Consumer's Data Right request in compliance with the timing provisions of C.R.S. § 6-1-1306(2)(a)-(b). A Controller does not have to comply with an authenticated Consumer request to access, correct, delete, or provide Personal Data in a portable format, to the extent that the Personal Data at issue meets the requirements of the exceptions in C.R.S. § 6-1-1307(1)(b) and 1307(3).

B. A Controller does not have to comply with an authenticated Consumer request to access, correct, delete, or provide Personal Data in a portable format, to the extent that the Personal Data at issue meets the requirements of the exceptions in C.R.S. § 6-1-1307(1)(b) and 1307(3).

C. If a Controller decides not to act on a Consumer's Data Right request, the Controller's response to the Consumer must include the grounds for denial, including but not limited to (1) any conflict with federal or state law; (2) if the Controller relied on an exception to the Colorado Privacy Act found at C.R.S. § 6-1-1304(2), a description of the exception; (3) the Controller's inability to Authenticate the Consumer's identity; (4) any factual basis for a Controller's good-faith claim that compliance is impossible; or (5) any basis for a good-faith, documented belief that the request is fraudulent or abusive.

1. If a Controller denies a Consumer Data Right request based on inability to Authenticate, the Controller must describe in documentation required by 4 CCR 904-3, Rule 6.11 their reasonable efforts to authenticate and why they were unable to do so.

2. A Controller that decides not to act on a Consumer's request must also provide instructions on how to appeal the Controller's decision in accordance with C.R.S. § 6-1- 1306(3).

D. When a Controller complies with a Consumer's Personal Data Right request, the Controller shall also use agreed upon technical, organizational, or other measures or processes, to instruct its Processors, pursuant to C.R.S. § 6-1-1305(2)(a), to fulfill requests relating to Personal Data held by the Processors.

E. Controllers must maintain all documentation as required by 4 CCR 904-3, Rule 6.11 of these rules.

F. If a Consumer or Authorized Agent submits a request to opt out of the Processing of a Consumer's Personal Data for an Opt-Out Purpose in a manner that is not one of the Controller's opt-out request methods, or submits a Data Right request that is otherwise deficient in a manner unrelated to the Authentication process, the Controller shall either: (1) treat the

request as if it had been submitted in accordance with the Controller's specified request methods, or (2) provide the Consumer or Authorized Agent that submitted the request with information on how to submit the request or remedy any deficiencies in the request.

PART 5 UNIVERSAL OPT-OUT MECHANISM

Rule 5.02 RIGHTS EXERCISED

A. Consumers may exercise their right to opt out of the Processing of Personal Data concerning the Consumer for purposes of Targeted Advertising or the Sale of Personal Data through a user- selected Universal Opt-Out Mechanism that meets the technical and other specifications provided in this Rule 5.

B. The purpose of a Universal Opt-Out Mechanism is to provide Consumers with a simple and easy- to-use method by which Consumers can automatically exercise their opt-out rights with all Controllers they interact with without having to make individualized requests with each Controller.

C. A Universal Opt-Out Mechanism may:

1. Express a Consumer's choice to opt out of the Processing of Personal Data for both the Processing of Personal Data for purposes of Targeted Advertising and Sale of Personal Data; or

2. Express a Consumer's choice to opt out of the Processing of Personal Data for only one specific purpose, either Targeted Advertising or Sale of Personal Data alone.

Rule 5.03 NOTICE AND CHOICE FOR UNIVERSAL OPT-OUT MECHANISMS

A. If a platform, developer, or provider provides a Universal Opt-Out Mechanism, that platform, developer, or provider shall make clear to the Consumer, whether in its configuration or disclosures to the public, that the mechanism is meant to allow the Consumer to exercise the right to opt out of the Processing of Personal Data for one specific purpose, either Targeted Advertising or Sale of Personal Data, or both purposes. These notices provided to the Consumer:

1. Shall comply with the requirements for disclosures and communications to Consumers provided in 4 CCR 904-3, Rule 3.02;

2. If applicable, shall state that the Universal Opt-Out Mechanism has been recognized by the Colorado Attorney General;

3. Shall clearly describe any limitations that may be applicable to the mechanism, for example:

   a. That the mechanism will allow a consumer to exercise the opt-out right for only one specific purpose, either Targeted Advertising or Sale of Personal Data; or

   b. That the mechanism applies only to a single browser or device.

4. Need not be tailored only to Colorado or refer to Colorado or to any other specific provisions of these rules or the Colorado Privacy Act, provided the mechanism meets the requirements of 4 CCR 904-3, Rule 5.03(A)(1)-(3).

   a. Example: A platform, developer, or provider discloses that its Universal Opt-Out Mechanism permits consumers to exercise "any and all opt-out rights available to you under state laws," and complies with the other requirements of this Rule 5.03(A) but makes no mention of Colorado nor recites any section of these rules or the Colorado Privacy Act. These disclosures satisfy the requirements of this Rule 5.03(A).

B. A valid Universal Opt-Out Mechanism must represent the Consumer's affirmative, freely given, and unambiguous choice to opt out of the Processing of Personal Data for the purposes listed at C.R.S. § 6-1-1306(1)(a)(IV)(A) and (B). Controllers are not obligated to honor Consumer rights requests for purposes other than those listed at C.R.S. § 6-1-1306(1)(a)(IV)(A) and (B) when transmitted through a Universal Opt-Out Mechanism.

C. The platform, developer, or provider that provides a Universal Opt-Out Mechanism is not obligated to authenticate that a user is a Resident of Colorado. The platform, developer, or provider may provide such authentication capabilities if it chooses.

Rule 5.04 DEFAULT SETTINGS FOR UNIVERSAL OPT-OUT MECHANISMS

A. To comply with C.R.S. § 6-1-1313(2), a Universal Opt-Out Mechanism may not be the default setting for a tool that comes pre-installed with a device, such as a browser or operating system.

1. Example: An operating system manufacturer bundles a browser pre-installed with every device shipped with the operating system. The browser sends a Universal Opt-Out mechanism signal by default and never asks the Consumer to enable this setting. The Consumer's decision to use this browser does not represent the Consumer's affirmative, freely given, and unambiguous choice to use the Universal Opt-Out Mechanism because it is a default choice. This is so even if the marketing for the operating system touts its privacy protective features.

2. Example: An operating system manufacturer bundles a browser and apps pre-installed with every device shipped with the operating system. The first time a Consumer runs a browser or app, the operating system asks the Consumer specifically and clearly whether they want to opt out of the Sale of their Personal Data using a Universal Opt-Out Mechanism signal when using the browser or app. No choice is pre-selected, meaning the Consumer is forced to decide. The Consumer's decision to select "yes" to enable the signal to opt out of the Sale of Personal Data represents the Consumer's affirmative, freely given, and unambiguous choice to use the Universal Opt-Out Mechanism.

B. Notwithstanding 4 CCR 904-3, Rule 5.04(A), a Consumer's decision to adopt a tool that does not come pre-installed with a device, such as a browser or operation system, but is marketed as a tool that will exercise a user's rights to opt out of the Processing of Personal Data using a Universal Opt-Out Mechanism, shall be considered the Consumer's affirmative, freely given, and unambiguous choice to use a Universal Opt-Out Mechanism. The marketing for such a tool may also describe functionality other than the exercise of opt out rights and it need not refer specifically to opt-out rights in the State of Colorado.

1. Example: A browser manufacturer markets its browser as a "privacy friendly" browser, prominently highlighting that the browser sends a Universal Opt-Out Mechanism signal by default. The browser does not come pre-installed with a device or operating system and must be installed by the Consumer. The Consumer's decision to use this browser represents the Consumer's affirmative, freely given, and unambiguous choice to use the Universal Opt-Out Mechanism. The Consumer need not be given an explicit choice about whether to use the Universal Opt-Out Mechanism in this example.

Rule 5.05 PERSONAL DATA USE LIMITATIONS

A. A platform, developer, or provider providing a Universal Opt-Out Mechanism shall not use, disclose, or retain any Personal Data collected from the Consumer in connection with the Consumer's utilization of the mechanism for any purpose other than sending or processing the opt-out preference. For example, the fact that a particular device sends a Universal Opt-Out Mechanism may not be used as part of a digital fingerprint to later identify that device.

B. When processing a Universal Opt-Out Mechanism, a Controller may not require the collection of additional Personal Data beyond that which is strictly necessary to authenticate a Consumer is a resident of Colorado determine that the mechanism represents a legitimate request to opt out of the Processing of Personal Data as permitted by C.R.S. § 6-1-1306(1)(a)(IV), or comply with the authentication mandates of the law of another jurisdiction specifically regarding universal opt-out mechanisms or signals.

Example: The law of a state other than Colorado obligates Controllers to gather specific pieces of information from a user before the Controller honors the use of a Universal Opt- Out Mechanism by that user. This additional information may be gathered while processing a Universal Opt-Out Mechanism, even if is not otherwise "strictly necessary to authenticate a Consumer is a resident of Colorado or determine that the mechanism represents a legitimate request".

C. Notwithstanding 4 CCR 904-3, Rule 5.05(B), a Controller may provide the Consumer with an option to provide additional Personal Data only if it will extend the recognition of the Consumer's use of the Universal Opt-Out Mechanism across platforms, devices, or offline. For example, a Controller may give the Consumer the option to provide their phone number or email address so that the Universal Opt-Out Mechanism or signal can apply to offline Sale of Personal Data or link the Consumer's opt-out choice across devices. Any information provided by the Consumer for this purpose shall not be used, disclosed, or retained for any purpose other than processing the opt-out request.

D. The Controller shall implement and maintain reasonable data security measures, consistent with 4 CCR 904-3, Rule 6.09, in Processing any Personal Data relating to the Consumer's use of a Universal Opt-Out Mechanism.

Rule 5.06 TECHNICAL SPECIFICATION

A. A Universal Opt-Out Mechanism must allow for Consumers to automatically communicate their opt-out choice with multiple Controllers.

1. The Universal Opt-Out Mechanism may communicate a Consumer's opt-out choice by sending an opt-out signal. The signal must be in a format commonly used and recognized by Controllers. An example would be an HTTP header field or JavaScript object.

B. The Universal Opt-Out Mechanism must allow Consumers to clearly communicate one or more opt-out rights available under C.R.S. § 6-1-1306(1)(a)(IV).

1. The Universal Opt-Out Mechanism may allow for a Consumer to opt out of Processing for one or more of the Opt-Out Purposes.

C. The Universal Opt-Out Mechanism must store, Process, and transmit any Consumer Personal Data using reasonable data security measures, consistent with 4 CCR 904-3, Rule 6.09.

D. A Universal Opt-Out Mechanism must not prevent the Controller's ability to determine:

1. Whether a Consumer is a Resident of the State of Colorado; or

2. That the Universal Opt-Out Mechanism represents a legitimate request to opt out of the Processing of Personal Data.

E. A Universal Opt-Out Mechanism must not unfairly disadvantage any Controller. For example, a Universal Opt-Out Mechanism may not engage in self-dealing benefiting the creator of the Universal Opt-Out Mechanism over other Controllers.

Rule 5.07 SYSTEM FOR RECOGNIZING UNIVERSAL OPT-OUT MECHANISMS

A. The Colorado Department of Law shall maintain a public list of Universal Opt-Out Mechanisms that have been recognized to meet the standards of this subsection. The initial list shall be released no later than January 1, 2024 and shall be updated periodically.

B. The goal of the public list is to simplify the options facing Controllers, Consumers, and other actors.

C. To be recognized, a Universal Opt-Out Mechanism must at a minimum meet these standards:

1. Comply with all of the technical and other specifications of Rule 5; and

2. Not create Consumer or Controller confusion about the similarities and differences between Universal Opt-Out Mechanisms on the public list.

D. The Colorado Department of Law may consider additional factors when determining which Universal Opt-Out Mechanisms to recognize. These include but are not limited to:

1. Commercial adoption by Consumers or Controllers;

2. Ease and cost of use, implementation, and detection by Consumers and Controllers;

3. Whether the Universal Opt-Out Mechanism has been approved by a widely recognized, legitimate standards body after broad multistakeholder participation in the standards- making process; and

4. Whether the Universal Opt-Out Mechanism is based on an open system or standard, and whether such standard is free for adoption by device, operating system, browser, and other manufacturers, Controllers, or Consumers without permission or on fair, reasonable, and non-discriminatory terms.

E. The public list shall describe recognized Universal Opt-Out Mechanisms in enough technical detail to permit Controllers to identify them when used by Consumers.

F. The Colorado Department of Law will allow Controllers six (6) months to recognize a Universal Opt-Out Mechanism once that Mechanism is added to the public list.

Rule 5.08 OBLIGATIONS ON CONTROLLERS

A. Effective July 1, 2024,

1. A Controller that receives an opt-out request through a Universal Opt-Out Mechanism shall treat such as a valid request to opt out of the Processing of Personal Data for purposes of Targeted Advertising, Sale of Personal Data, or both purposes, as indicated by the mechanism, for the associated browser or device, and, if known, for the Consumer.

2. After receiving a valid opt-out request through the use of a Universal Opt-Out Mechanism, a Controller shall continue to treat the browser, device, and Consumer as having exercised opt-out rights until the Consumer Consents to the Sale of Personal Data or Processing of Personal Data for Targeted Advertising, as specified in 4 CCR 904-3, Rule 5.09.

3. A Controller shall be capable of recognizing any Universal Opt-Out Mechanism reflected in the public list maintained by the Colorado Department of Law pursuant to subsection 4 CCR 904-3, Rule 5.07 provided the Controller has had at least six months' notice of the addition of new mechanisms. For example, in the case of a recognized Universal Opt-Out Mechanism sent as a signal, the Controller must listen for the signal.

B. A Controller may also recognize Universal Opt-Out Mechanisms that are not reflected in the public list maintained by the Colorado Department of Law pursuant to subsection 4 CCR 904-3, Rule 5.07.

C. Notwithstanding 4 CCR 904-3, Rule 5.08(A), a Controller may choose to honor an opt-out request received through a Universal Opt-Out Mechanism prior to July 1, 2024, pursuant to C.R.S. § 6-1- 1306(a)(IV)(A).

D. Unless a Controller is Authenticating a Consumer as permitted by C.R.S. § 6-1-1313(2)(f), a Controller may not require a Consumer to login or otherwise Authenticate themself as a condition of recognizing the Consumer's use of a Universal Opt-Out Mechanism. A Controller may not subject a Consumer to undertake any authentication actions that are unnecessary or unnecessarily burdensome.

E. A Controller may display in a conspicuous manner if it has Processed the Consumer's opt-out preference signal. For example, the Controller may display on its website "Opt-Out Preference Signal Honored" when a browser, device, or Consumer utilizing a Universal Opt-Out Mechanism visits the website.

F. Pursuant to C.R.S. § 6-1-1313(2)(f), a Controller may authenticate that the user sending an opt- out request through a Universal Opt-Out Mechanism is a Resident of Colorado, but they are not obligated to do so.

Rule 5.09 CONSENT AFTER UNIVERSAL OPT-OUT

A. A Controller may enable a Consumer to Consent to Processing that the Consumer has opted-out of using a Universal Opt-Out mechanism, so long as the Controller's request for Consent complies with the Consent requirements provided in C.R.S. § 6-1-1306(1)(a)(IV)(C), and 4 CCR 904-3, Rule 7.05.

B. A Controller shall not interpret the absence of a Universal Opt-Out Mechanism signal after the Consumer previously utilized a Universal Opt-Out Mechanism as Consent to opt back in.

PART 6 DUTIES OF CONTROLLERS

Rule 6.02 PRIVACY NOTICE PRINCIPLES

A. A privacy notice shall provide Consumers with a meaningful understanding and accurate expectations of how their Personal Data will be Processed. It shall also inform Consumers about their rights under the Colorado Privacy Act and provide any information necessary for Consumers to exercise those rights.

B. A Controller is not required to provide a separate Colorado-specific privacy notice or section of a privacy notice as long as the Controller's privacy notice meets all requirements of this section and makes clear that Colorado Consumers are entitled to the rights provided by C.R.S. § 6-1-1306.

C. A privacy notice shall comply with all requirements for disclosures and communications to Consumers provided in 4 CCR 904-3, Rule 3.02.

D. A privacy notice must be clear. Information contained in a privacy notice shall be:

1. Concrete and definitive, avoiding abstract or ambivalent terms that may lead to varying interpretations.

2. Clearly labeled, such that Consumers seeking to understand a Controller's Processing activities or how to exercise their Data Rights can easily access the section of the privacy notice containing relevant information.

E. A privacy notice must be easily accessible. A privacy notice must be:

1. Posted online through a conspicuous link using the word "privacy" on the Controller's website homepage or on a mobile application's app store page or download page. A Controller that maintains an application on a mobile or other device shall also include a link to the privacy notice in the application's settings menu.

   a. A Controller that does not operate a website shall make the privacy notice conspicuously available to Consumers through a medium regularly used by the Controller to interact with Consumers. For instance, if a Controller interacts with a Consumer offline, an offline version of the privacy notice must be available to the Consumer.

F. A privacy notice must be specific. The level of specificity in a privacy notice should enable a Consumer to understand, in advance or at the time of the Processing, the scope of the Controller's Processing operations, such that a Consumer should not be taken by surprise at a later point about Personal Data that has been collected and the ways in which Personal Data has been Processed.

Rule 6.03 PRIVACY NOTICE CONTENT

A. A privacy notice must include the following information:

1. A comprehensive description of the Controller's online and offline Personal Data Processing practices, including but not limited to the following, linked in a way that gives Consumers a meaningful understanding of how each category of their Personal Data will be used when they provide that Personal Data to the Controller for a specified purpose:

   a. The categories of Personal Data Processed, including, but not limited to, whether Personal Data of a Child or other Sensitive Data is Processed.

      i. Categories shall be described in a level of detail that provides Consumers a meaningful understanding of the type of Personal Data Processed. For example, categories of Personal Data described at a sufficiently granular level of detail include, but are not limited to: "contact information," "government issued identification numbers," "payment information", "Information from Cookies," "data revealing religious affiliation," and "medical data."

   b. The Processing purpose described in a level of detail that gives Consumers a meaningful understanding of how each category of their Personal Data is used when provided for that Processing purpose.

   c. Whether the Personal Data provided for a specific purpose will be sold or used for Targeted Advertising or Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer.

   d. Categories of Personal Data that the Controller Sells to or shares with Third Parties, if any.

   e. Categories of Third Parties to whom the Controller sells, or with whom the Controller shares Personal Data, if any. Categories of Third Parties must be described in a level of detail that gives Consumers a meaningful understanding of the type of, business model of, or processing conducted by the Third Party.

      i. For example, categories of Third Parties described in a sufficiently granular level of detail include, but are not limited to: "analytics companies," "data brokers," "third-party advertisers," "payment processors," "lenders," "other merchants," and "government agencies."

2. If a Controller's Processing activity involves the Processing of Personal Data for the purpose of Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer, all disclosures required by 4 CCR 904-3, Rule 9.03.

3. A list of the Data Rights available.

4. A description of the methods through which a Consumer may submit requests to exercise Data Rights, as required by C.R.S. § 6-1-1306(1) and 4 CCR 904-3, Rule 4.02, including:

   a. Instructions on how to use each method.

   b. Instructions on how an Authorized Agent may submit a request to opt out of the Processing of Consumer Personal Data on a Consumer's behalf pursuant to C.R.S. § 6-1-1306(1)(a)(II).

   c. A clear and conspicuous method to exercise the right to opt out of the Processing of Personal Data concerning the Consumer pursuant to C.R.S. § 6-1- 1306(1)(a)(I) and (1)(a)(III), or links to any online method, such as a webform or portal, consistent with 4 CCR 904-3, Rule 4.03.

   d. A description of the commercially reasonable process the Controller uses to Authenticate the identity of a Consumer exercising a Data Right request or to Authenticate the authority of an Authorized Agent exercising the right to opt out on a Consumer's behalf.

e. Effective July 1, 2024, an explanation of how requests to opt out using Universal Opt-Out Mechanisms will be processed.

5. If a Controller will delete Sensitive Data Inferences within twenty-four (24) hours pursuant to 4 CCR 904-3, Rule 6.10, a description of the Sensitive Data Inferences subject to this provision and the retention and deletion timeline for such Sensitive Data Inferences.

6. A Controller's contact information.

7. Instructions on how a Consumer may appeal a Controller's action in response to the Consumer's request, as contemplated by C.R.S. § 6-1-1306(3).

8. The date the privacy notice was last updated.

Rule 6.04 CHANGES TO A PRIVACY NOTICE

A. A Controller shall notify Consumers of material changes to a privacy notice. Such changes to a privacy notice shall be communicated to Consumers in a manner by which the Controller regularly interacts with Consumers.

1. Material changes may include, but are not limited to, changes to: (1) categories of Personal Data Processed; (2) Processing purposes; (3) a Controller's identity; (4) the act of sharing of Personal Data with Third Parties; (5) categories of Third Parties Personal Data is shared with; or (6) methods by which Consumers can exercise their Data Rights request.

B. If a material change rises to the level of a secondary use, a Controller must obtain Consent from a Consumer pursuant to 4 CCR 904-3, Rules 7.02-7.05 in order to Process Personal Data that was collected before the change to the privacy notice for that Secondary Use.

Rule 6.05 LOYALTY PROGRAMS

A. Pursuant to 6-1-1308(1)(d), a Controller is not prohibited from offering Bona Fide Loyalty Program Benefits to a Consumer based on the Consumer's voluntary participation in a Bona Fide Loyalty Program.

B. If a Consumer exercises their right to delete Personal Data such that it is impossible for the Controller to provide a certain Bona Fide Loyalty Program Benefit to the Consumer, the Controller is no longer obligated to provide that Bona Fide Loyalty Benefit to the Consumer. However, the Controller shall provide any available Bona Fide Loyalty Program Benefit for which the deleted Personal Data is not necessary.

C. If a Consumer exercises their right to opt out of the Sale of Personal Data or Processing of Personal Data for Targeted Advertising, such that the exchange of Personal Data needed to obtain a Bona Fide Loyalty Program Benefit through a Bona Fide Loyalty Program Partner is no longer possible, the Controller is no longer obligated to provide that Bona Fide Loyalty Program Benefit to the Consumer.

1. If the Controller's Bona Fide Loyalty Program offers Bona Fide Loyalty Program Benefits that are unrelated to the exchange of Personal Data with a Bona Fide Loyalty Program Partner, the Controller shall continue to provide those Benefits to a Consumer who opts out of the Sale of Personal data or Processing of Personal Data for Targeted Advertising.

2. The sale of Personal Data or Processing of Personal Data for Targeted Advertising that is unrelated to sharing of information with a Bona Fide Loyalty Program Partner is a Secondary Use that requires Consent pursuant to 4 CCR 904-3, Rule 6.08.

D. If a Consumer refuses to Consent to the Processing of Sensitive Data necessary for a personalized Bona Fide Loyalty Program Benefit, the Controller is no longer obligated to provide that personalized Bona Fide Loyalty Program Benefit. However, the Controller shall provide any available, non-personalized Bona Fide Loyalty Program Benefit for which the Sensitive Data is not necessary. A Controller may not condition a Consumer's participation in a Bona Fide Loyalty Program on the Consumer's Consent to Process Sensitive Data unless the Sensitive Data is required for all Bona Fide Loyalty Program Benefits.

E. If a Consumer's decision to exercise a Data Right impacts the Consumer's membership in a Bona Fide Loyalty Program, the Controller shall notify the Consumer of the impact of the Consumer's decision in conformance with 4 CCR 904-3, Rule 3.02 and at least twenty-four (24) hours before discontinuing the Consumer's Bona Fide Loyalty Program Benefit or membership, and must provide a reference or link to the information required by subparagraph F, below.

F. Loyalty Program Disclosures

1. In addition to all other disclosures required by 4 CCR 904-3, Rules 6.03 and 7.03, a Controller maintaining a Bona Fide Loyalty Program must provide the following disclosures at the point of program registration, either directly, or in the form of a link to the specific section of a privacy notice or terms and conditions containing such information:

    a. The categories of Personal Data or Sensitive Data collected through the Bona Fide Loyalty Program that will be Sold or Processed for Targeted Advertising, if any;

    b. Categories of Third Parties that will receive the Consumer's Personal Data and Sensitive Data, provided in the level the detail described in 4 CCR 904-3, Rule 6.03(a)(1)(e), including whether Personal Data will be provided to Data Brokers;

    c. A list of any Bona Fide Loyalty Program Partners, and the Bona Fide Loyalty Program Benefits provided by each Bona Fide Loyalty Program Partner.

    d. If a Controller claims that a Consumer's decision to delete Personal Data makes it impossible to provide a Bona Fide Loyalty Program Benefit, then the Controller shall provide an explanation of why the deletion of Personal Data makes it impossible to provide a Bona Fide Loyalty Program Benefit.

    e. If a Controller claims that a Consumer's Sensitive Data is required for a Bona Fide Loyalty Program Benefit, then the Controller shall provide an explanation of why the Sensitive Data is required for a Bona Fide Loyalty Program Benefit.

2. Bona Fide Loyalty Program terms and requests for Consent to Process Sensitive Data or Personal Data in connection with the Bona Fide Loyalty Program shall also include a link to the Controller's privacy notice.

G. Example: A Consumer joins a grocery store's Bona Fide Loyalty Program that includes both personalized and non-personalized Bona Fide Loyalty Program Benefits. The grocery store asks the Consumer for Consent to collect Sensitive Data about the Consumer in order to provide personalized Bona Fide Loyalty Program Benefits. When the Consumer refuses Consent, the Controller gives timely notice to the Consumer that it will not provide the personalized Bona Fide Loyalty Program Benefits, but will continue to provide non-personalized Bona Fide Loyalty Program Benefits. Moving forward, the Controller provides only the non-personalized Bona Fide Loyalty Program Benefits following the Consumer's decision to continue to refuse Consent to the collection of Sensitive Data. The Controller is not acting impermissibly because the grocery store is still providing all available non-personalized Bona Fide Loyalty Program Benefits and did not condition the Consumer's participation in the Bona Fide Loyalty Program on the Consumers Consent to process Sensitive Data that is not required for personalized Bona Fide Loyalty Program Benefits.

H. Example: A Consumer joins a hotel chain's Bona Fide Loyalty Program, which provides points that can be applied to obtain discounts for that hotel chain, and for a popular restaurant chain that is not otherwise affiliated with the hotel chain. The restaurant chain requires the hotel chain to provide the Personal Data of each Consumer who wishes to apply the hotel chain's points to obtain restaurant discounts. When the Consumer opts out of the Sale of Personal Data and Processing of Personal Data for Targeted Advertising, the Controller is unable to provide the required information to the restaurant

chain. The Controller may discontinue the Bona Fide Loyalty Program Benefit that allows Consumers to use points for discounts for the restaurant chain. However, the hotel chain must still provide all available Bona Fide Loyalty Benefits to be used at the hotel chain.

I. Example: A Consumer joins a retailer's Bona Fide Loyalty Program that offers discounts on products based on the Consumer's purchase history. The retailer wishes to fund the loyalty program, in part, by selling the Consumer's purchase history to a Data Broker. The retailer must obtain the Consumer's consent to Sell the Consumer's Personal Data to the Data Broker because selling Personal Data obtained through a Bona Fide Loyalty Program to a Data Broker is a secondary use.

J. Example: A Consumer exercises their right to opt out of the Processing of Personal Data for Targeted Advertising. An online gaming company gives the Consumer fewer free games through the company's service, arguing that the additional free games are for members of its loyalty program, which requires the use of Personal Data for Targeted Advertising. The company's differential treatment is prohibited if the Processing of Personal Data is not necessary to provide the additional games. However, if the free games are provided by a Bona Fide Loyalty Program Partner that requires the Consumer data for Targeted Advertising through a co-marketing agreement with the Controller, the differential treatment may be appropriate.

Rule 6.06 PURPOSE SPECIFICATION

A. Controllers shall specify the express purposes for which each category of Personal Data is collected and Processed in both external disclosures to Consumers, including privacy notices required by C.R.S. § 6-1-1308(1), as well as in any internal documentation required by this Part 6.

B. The express purpose must be described in a level of detail that gives Consumers a meaningful understanding of how each category of their Personal Data is used when provided for that Processing purpose.

C. If Personal Data is collected and Processed for more than one purpose, Controllers should specify each unrelated purpose with enough detail to allow Consumers to understand each individual, unrelated purpose.

1. Controllers should not identify one broad purpose to justify numerous Processing activities that are only remotely related.

2. Controllers should not specify one broad purpose to cover potential future Processing activities that are only remotely related.

3. Controllers should not specify so many purposes for which Personal Data could potentially be processed to cover potential future processing activities that the purpose becomes unclear or uninformative.

D. If the Processing purpose has evolved beyond the original express purpose such that it becomes a distinct purpose that is no longer reasonably necessary to or compatible with the original express purpose, the Controller must review and update all related disclosures and documentation as necessary.

Rule 6.07 DATA MINIMIZATION

A. To ensure all Personal Data collected is reasonably necessary for the specified purpose, Controllers shall carefully consider each Processing purpose and determine the minimum Personal Data that is necessary, adequate, or relevant for the express purpose or purposes.

B. Personal Data should only be kept in a form which allows identification of Consumers for as long as is necessary for the express Processing purpose(s). To ensure that the Personal Data are not kept longer than necessary, adequate, or relevant, Controllers shall set specific time limits for erasure or to conduct a periodic review.

1. Any Personal Data determined to no longer be necessary, adequate, or relevant to the express Processing purpose(s) shall be deleted by the Controller and any Processors that the Controller has shared the Personal Data with.

2. Biometric Identifiers, a digital or physical photograph of a person, an audio or voice recording containing the voice of a person, or any Personal Data generated from a digital or physical photograph or an audio or video recording held by a Controller shall be reviewed at least once a year to determine if its storage is still necessary, adequate, or relevant to the express Processing purpose. Such assessment shall be documented according to 4 CCR 904-3, Rule 6.11.

3. Sensitive Data for which Controllers no longer have consent to Process, should be deleted or otherwise rendered permanently anonymized or inaccessible within a reasonable period of time after withdrawal of Consent.

C. A Controller shall not collect Personal Data other than those disclosed in its required privacy notice. If the Controller intends to collect additional Personal Data the Controller shall revise its privacy notice, and notify Consumers of the change to its privacy notice pursuant to 4 CCR 904-3, Rule 6.04.

Rule 6.08 SECONDARY USE

A. The specified Processing purpose is the purpose disclosed to Consumers at or before the time the Personal Data is collected or processed from Consumers. Such disclosure shall be included in any required privacy notice or Consent disclosure.

B. Before Processing Personal Data for purposes that are not reasonably necessary to or compatible with specified Processing purpose(s) disclosed on or after July 1, 2023, the Controller must obtain Consent consistent with C.R.S. § 6-1-1308 and 4 CCR 904-3, Rules 7.02-7.05.

C. When considering if the new Processing purpose is reasonably necessary to or compatible with the original specified purpose(s), Controllers may consider the following, as applicable:

1. The reasonable expectation of an average Consumer concerning how their Personal Data would be Processed once it was collected;

2. The link between the original specified purpose(s) for which the data was collected and the purpose(s) of further Processing;

3. The relationship between the Consumer and the Controller and the context in which the Personal Data was collected;

4. The type, nature, and amount of the Personal Data subject to the new Processing purpose;

5. The type and degree of possible consequence or impact to the Consumer of the new Processing purpose;

6. The identity of the entity conducting the new Processing purposes, e.g., the same or different Controller, or a Third Party; and

7. The existence of additional safeguards for the Personal Data, such as encryption or pseudonymization.

Rule 6.09 DUTY OF CARE

A. Personal Data must be Processed in a manner that ensures reasonable and appropriate administrative, technical, organizational, and physical safeguards of Personal Data collected, stored, and Processed.

B. When determining reasonable and appropriate safeguards, Controllers should consider:

1. Applicable industry standards and frameworks;

2. The nature, size, and complexity of the Controller's organization;

3. The sensitivity and amount of Personal Data;

4. The original source of Personal Data;

5. The risk of harm to Consumers resulting from unauthorized or unlawful access, use, or degradation of the Personal Data; and

6. The burden or cost of safeguards to protect Personal Data from harm assessed in 4 CCR 904-3, Rule 6.09(B)(5).

C. Reasonable and appropriate administrative, technical, organizational, and physical safeguards must be designed to:

1. Protect against unauthorized or unlawful access to or use of Personal Data and the equipment used for the Processing and against accidental loss, destruction, or damage;

2. Ensure the confidentiality, integrity, and availability of Personal Data collected, stored, and Processed;

3. Identify and protect against reasonably anticipated threats to security or the integrity of information; and

4. Oversee compliance with data security policies by the Controller and Processors through reasonable requirements.

D. Reasonable and appropriate administrative, technical, organizational, and physical safeguards to secure Personal Data include but are not limited to those measures provided by C.R.S. § 6-1-713.5 and C.R.S. § 24-73-102, as interpreted by state courts and administrative orders.

Rule 6.10 DUTY REGARDING SENSITIVE DATA

A. Controllers must obtain Consent to Process Sensitive Data, including Sensitive Data Inferences, consistent with C.R.S. § 6-1-1308(7) and 4 CCR 904-3, Rules 7.02-7.05.

B. Controllers may be exempt from obtaining Consent to Process Sensitive Data Inferences from Consumers over the age of thirteen (13) only if:

1. The Processing purpose of such Personal Data would be obvious to a reasonable Consumer based on the context of the collection and use of the Personal Data, and the relationship between the Controller and Consumer;

2. Sensitive Data Inferences are permanently deleted within twenty-four (24) hours of collection or of the completion of the Processing activity, whichever comes first;

3. Sensitive Data Inferences are not transferred, sold, or shared with any Processors, Affiliates, or Third-Parties; and

4. The Personal Data and any Sensitive Data Inferences are not Processed for any purpose other than the express purpose disclosed to the Consumer.

C. If a Controller will delete Sensitive Data Inferences within twenty-four (24) hours, pursuant to this section, they must (1) include description of the Sensitive Data Inferences subject to this provision and the retention and deletion timeline for such Sensitive Data Inferences in its privacy notice, pursuant to 4 CCR 904-3, Rule 6.03, and (2) include the details of the deletion and verification process in the Controller's Data Protection Assessment, pursuant to 4 CCR 904-3, Rule 8.04.

Rule 6.11 DOCUMENTATION CONCERNING DUTIES OF CONTROLLERS

A. Controllers shall maintain records of all Consumer Data Rights requests made pursuant to C.R.S. § 6-1-1306 for at least twenty-four (24) months. Such records shall include, at a minimum, each of the following:

1. The date of request;

2. The Consumer Data Rights request type;

3. The date of the Controller's response;

4. The nature of the Controller's response;

5. The basis for the denial of the request if the request is denied in whole or in part; and

6. The existence and resolution of any Consumer appeal to a denied request.

B. Controllers shall maintain a record of all Data Rights requests made pursuant to C.R.S. § 6-1- 1306 with which the Controller has previously complied. Such records shall be retained for at least twenty-four (24) months and shall be made available at the completion of a merger, acquisition, bankruptcy, or other transaction in which a Third Party assumes control of Personal Data to ensure any new Controller continues to recognize the Consumer's previously exercised Data Rights.

C. Controllers shall maintain documents sufficient to demonstrate compliance with 4 CCR 904-3, Rules 6.07, 6.08, and 7.06 for as long as the Processing activity continues, and for at least twenty-four (24) months after the conclusion of Processing activity.

D. Required records shall be maintained in a readable format, appropriate to the sophistication and size of the Controller's business.

E. The Controller shall implement and maintain reasonable security procedures and practices, consistent with 4 CCR 904-3, Rule 6.09, in maintaining all required records.

F. Personal Data maintained pursuant to this 4 CCR 904-3, Rule 6.11, where that information is not used for any other purpose, shall not be subject to Data Rights requests.

G. Personal Data maintained for required documentation shall not be used for any other purpose except as reasonably necessary for the business to review and modify its processes for compliance with the Colorado Privacy Act, C.R.S. § 6-1-1301, *et seq*., and these rules. Personal Data maintained for required documentation shall not be shared with any Third Party except as necessary to comply with a legal obligation or as part of a merger, acquisition, bankruptcy, or other transaction in which a Third Party assumes control of Personal Data.

H. Other than as required by this subsection and 4 CCR 904-3, Rule 4.06, a Controller is not required to retain Personal Data solely for the purpose of fulfilling a Data Rights request made under the Colorado Privacy Act, C.R.S. § 6-1-1301, *et seq*.

PART 7 CONSENT

Rule 7.02 REQUIRED CONSENT

A. Pursuant to C.R.S. §§ 6-1-1303(5), 6-1-1306(1)(a)(IV)(C), 6-1-1308(4), and 6-1-1308(7), a Controller must obtain valid Consumer Consent prior to:

1. Processing a Consumer's Sensitive Data;

2. Processing Personal Data concerning a known Child, in which case the Child's parent or lawful guardian must provide Consent;

3. Selling a Consumer's Personal Data, Processing a Consumer's Personal Data for Targeted Advertising, or Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer after the Consumer has exercised the right to opt out of the Processing for those purposes; and

4. Processing Personal Data for purposes that are not reasonably necessary to, or compatible with, the original specified purposes for which the Personal Data are Processed.

B. Controllers may rely upon valid consent obtained prior to July 1, 2023, to continue to Process a Consumer's previously collected Personal Data, including Sensitive Data, collected before July 1, 2023. Consent obtained before July 1, 2023, shall be considered valid only if it would comply with the requirements set forth in C.R.S. §§ 6-1-1303(5), 6-1-1306(1)(a)(IV)(C), 6-1-1308(4), and 6-1- 1308(7) and Part 7 of these rules.

1. Controllers that do not obtain valid Consent prior to July 1, 2023 to continue to use, store, or otherwise Process Sensitive Data collected prior to this date must obtain valid Consent, as required by C.R.S. §§ 6-1-1303(5), 6-1-1306(1)(a)(IV)(C), 6-1-1308(4), and 6-1-1308(7) and Part 7 of these rules, by July 1, 2024 to continue to Process the previously collected Sensitive Data.

2. If a Controller has collected Personal Data prior to July 1, 2023 and the Processing purpose changes after July 1, 2023 such that it is considered a secondary use pursuant to C.R.S. § 6-1-1308(4) and 4 CCR 904-3, Rule 6.08, the Controller must obtain valid Consent, as required by C.R.S. §§ 6-1-1303(5), 6-1-1306(1)(a)(IV)(C), 6-1-1308(4), and 6-1-1308(7) and Part 7 of these rules, at the time the Processing purpose changes to continue to Process the previously collected Personal Data.

C. Notwithstanding the above, a Controller Processing Sensitive Data Inferences is not required to obtain Consent for the Processing activity if the Processing falls within the requirements of 4 CCR 904-3, Rule 6.10.

Rule 7.03 REQUIREMENTS FOR VALID CONSENT

A. To be valid, a Consent must meet each of the following elements: (1) it must be obtained through the Consumer's clear, affirmative action; (2) it must be freely given by the Consumer; (3) it must be specific; (4) it must be informed; and (5) it must reflect the Consumer's unambiguous agreement.

B. Consent must be obtained through the Consumer's clear, affirmative action. For purposes of obtaining valid Consent:

1. A "clear, affirmative action" means a Consumer's Consent is communicated through either (a) deliberate and clear conduct, or (b) a statement that clearly indicates their acceptance of the proposed Processing of their Personal Data.

2. A blanketed acceptance of general terms and conditions, silence, inactivity or in action, pre-ticked boxes, and other negative option opt-out constructions that require intervention from the Consumer to prevent agreement are not clear affirmative actions for the purposes of valid Consent.

C. Consent must be freely given. For purposes of obtaining valid Consent:

1. Consent is freely given when Consumers may refuse Consent without detriment and withdraw Consent easily at any time.

2. Consent is not freely given when:

    a. It reflects acceptance of a general or broad terms of use or similar document that contains descriptions of Personal Data Processing along with other, unrelated information;

    b. The performance of a contract is dependent on Consent to Process Personal Data that is not necessary to provide the goods or services contemplated by the contract; or

    c. The Controller denies goods, services, discounts, or promotions to a Consumer who chooses not to provide Consent, unless:

        i. The Personal Data is necessary to the provision of those goods, services, discounts, or promotions, consistent with 4 CCR 904-3, Rule 6.05; or

        ii. The Consent is otherwise required in connection with a Consumer's voluntary participation in a Bona Fide Loyalty Program, consistent with the requirements in 4 CCR 904-3, Rule 6.05.

3. Example: An online dating application's terms and conditions tells users that the application will disclose collected Personal Data, including Sensitive Data revealing sexual orientation, with similar applications for advertising purposes. Consent is required for the disclosure of Sensitive Data with similar applications for advertising purposes. Since users cannot accept the required terms and conditions without the opportunity to separately provide or withhold Consent for sharing with similar applications, the Consent is not freely given.

D. Consent must be specific.

1. When Controllers request Consent to Process Personal Data for more than one Processing purpose, and those Processing purposes are not reasonably necessary to or compatible with one another, Consumers must have the ability to separately Consent to each specific purpose.

    a. Controllers may request Consent to Process Personal Data for multiple Processing purposes that are not reasonably necessary to or compatible with one another using a single Consent request as long there is also an option for more granular Consent within the same Consent interface.

2. Consent to Process Personal Data for one specific purpose does not constitute valid Consent to Process Personal Data for other purposes that are not reasonably necessary to or compatible with that specific purpose.

3. The Sale of Sensitive Data to one specific party is not necessary to or compatible with the Sale of Sensitive Data to a different party.

    a. Example: A cosmetic retailer asks a customer for Consent to use Sensitive Data revealing the customer's racial origin in order to provide first-party targeted offers to the customer and to Sell the customer's racial origin information to Data Brokers. This Consent is not specific as there is no opportunity to provide separate Consent for the two separate Processing purposes. Therefore, Consent in this example would not be valid.

    b. Example: In the example above, the Controller requests Consent only to Sell Sensitive Data revealing the customer's racial origin with commercial partners. The Controller lists "Fashion Co. #1" and "Make Up Co. #1" as commercial partners who will receive Sensitive Data. Consent would be deemed valid for only these two Third Parties because their identity was provided to the Consumer at the time that his or her Consent was collected. Consent would not be deemed valid for Selling with another Third Party whose identity has not been provided.

E. Consent must be informed.

1. When requesting Consent, a Controller must provide the following information, at a minimum:

a. The Controller's identity;

b. The plain-language reason that Consent is required;

c. The Processing purpose(s) for which Consent is sought;

d. The categories of Personal Data that the Controller shall Process to effectuate the Processing purpose(s);

e. Names of all Third Parties receiving the Sensitive Data through Sale, if applicable;

f. A description of the Consumer's right to withdraw Consent for the identified Processing purpose at any time in accordance with 4 CCR 904-3, Rule 7.07 and details of how and where to do so; and

g. Any disclosures required by 4 CCR 904-3, Rules 6.05 and 9.05.

F. Consent may not be obtained using Dark Patterns as defined in C.R.S § 6-1-1309(9) and prohibited by 4 CCR 904-3, Rule 7.09. Pursuant to C.R.S. § 6-1-1303(5)(c) and 4 CCR 904-3, Rule 7.09, any agreement obtained through Dark Patterns is not valid Consent.

Rule 7.04 REQUESTS FOR CONSENT

A. Controllers shall provide a simple form or mechanism to enable a Consumer to provide Consent when required, including Consent to Processing purposes from which the Consumer has previously opted out. Such a form or mechanism should be easy for a reasonable Consumer to locate and should comply with the other requirements set forth in Part 7 of these rules.

B. Requests for Consent shall be prominent, concise, and separate and distinct from other terms and conditions, and shall comply with all requirements for disclosures and communications to Consumers set forth in 4 CCR 904-3, Rule 3.02.

C. Any Consent request by a Controller must contain the disclosures required by 4 CCR 904-3, Rule 7.03(E)(1) either directly or through a link. Where possible, the request interface itself should contain the disclosures required by 4 CCR 904-3, Rule 7.03(E)(1)(a)-(d). Alternatively, the Controller may provide the Consumer with a link to a webpage containing the required Consent disclosures, provided the request clearly states the title and heading of the webpage section containing the relevant disclosures. If technically feasible, the request method must also link the Consumer directly to the relevant section of the disclosure.

D. Example: A mobile application requests Consent to Process Sensitive Data. The Consent request provides a link to the application's privacy notice which contains the required Consent disclosures. However, the Consent request does not direct or bring the Consumer to the relevant section of the privacy notice. Consent is not valid because the Consent request does not clearly indicate the title and section where the Consumer can find the required disclosures and did not link the Consumer directly to the relevant section of the privacy notice.

E. Example: Acme Toy Store collects customer email addresses in order to send customers information about product recalls, and maintains those email addresses in a recall email distribution list. Acme Toy Store wants to Sell the recall email distribution list to a Third Party partner to enable that partner to send those customers promotional materials. Acme Toy Store must obtain customer consent prior to Selling the recall email distribution list because Selling the recall email distribution list is not reasonably necessary to or compatible with providing product recall information. Acme Toy Store emails its customers attaching a revised privacy notice disclosing the new Processing purpose and asks customers to

Consent to the new privacy notice, but does not state the new purpose in the email, and does not direct customers to the section of the privacy notice disclosing the secondary purpose. Consent is not valid because the email did not contain the required Consent disclosures or direct the customers to a document containing the required Consent disclosures.

1. Example: Under the same circumstances, Acme Toy Store emails its customers on the recall distribution list informing those customers that Consent is required for the Acme Toy Store to Process email addresses for the secondary purpose of Selling the recall distribution list to a Third Party partner to enable that partner to send promotional materials, providing all other required disclosures and including a mechanism that enables the customers to provide Consent and to revoke Consent through the same user interface. Consent is valid because the email contained all required Consent disclosures in an acceptable form.

2. Example: Under the same circumstances, Acme Toy Store emails the product recall email distribution list informing those customers that it would like to use their email addresses for the secondary purpose of Selling the recall distribution list to a Third Party partner as contemplated in section B.2.e. of its privacy notice, explains that it cannot use the customers' email addresses for that secondary purpose without their consent, and requests the customers' Consent to Process their email address for that secondary purpose. It then provides a link directly to section B.2.e. of its privacy notice which explains that Acme Toy Store Sells customer email addresses, including those Processed for the purpose of product recall notifications, to marketing partners, in addition to all other disclosures. The email provides a Consent mechanism that enables the customers to provide or revoke consent through the same user interface. Consent is valid because the email and linked page together contained all required disclosures, the email provided the specific section of the relevant disclosures, and the link brought the customers directly to the relevant disclosures.

Rule 7.05 CONSENT AFTER OPT-OUT

A. The Consumer's decision to Consent to Processing activities from which the Consumer has previously opted-out using either a Universal Opt-Out Mechanism or directly with a particular Controller is subject to the requirements for Consent under 4 CCR 904-3, Rules 7.03 and 7.04.

B. A Controller that wishes to obtain Consent to Process Personal Data for an Opt-Out Purpose after the Consumer has opted out of Processing for that Purpose shall not request Consent using schemes that cause consent fatigue, such as interface dominating cookie banners, high frequency requests, cookie walls, pop-ups, or other any other interstitials that degrade or obstruct the Consumer's experience on the Controller's web page or application.

1. A Controller may proactively request Consent to Process Personal Data for an Opt-Out Purpose after the Consumer has opted out, by providing a link to a privacy settings page, menu, or similar interface, or comparable offline method, that enables the Consumer to Consent to the Controller Processing the Personal Data for the Opt-Out Purpose, so long as the request for Consent meets all other requirements for valid Consent under this Part 7.

2. If a Controller has a reasonable belief that a Consumer intended to opt back into the Sale of Personal Data or Processing of Personal Data for Targeted Advertising, the Controller may proactively send a link to a privacy settings page or other method to enable the Consumer to Consent to the Controller Processing the Personal Data for the Opt-Out Purpose directly to a Consumer.

C. If a Controller conspicuously displays the status of the Consumer's opt-out choice on the website pursuant to 4 CCR 904-3, Rule 5.08(E), the link to provide Consent may appear beside or in conjunction with the Consumer's opt-out status.

D. If a Consumer has opted-out of the Processing of Personal Data for the Opt-Out Purposes, and then initiates a transaction or attempts to use a product or service inconsistent with the request to opt-out, such as signing up for a Bona Fide Loyalty Program that also involves the Sale of Personal Data to a Bona Fide Loyalty Program Partner, the Controller may request the Consumer's Consent to Process the Consumer's Personal Data for that purpose, so long as the request for Consent complies with all provisions of 4 CCR 904-3, Rules 7.03 and 7.04.

E. Example: A Consumer opts out of the use of Personal Data for Sale or Targeted Advertising using a Universal Opt-Out Mechanism. The Consumer visits the website of a fashion retailer that routinely shares Consumer Personal Data for Targeted Advertising. The fashion retailer must obtain the Consumer's consent because the Consumer has already opted out of Processing for that purpose. The fashion retailer's website displays a pop-up banner seeking Consent to share the Consumer's Personal Data for Targeted Advertising. This is not a valid request for Consumer Consent because the request is made through a pop-up banner that degrades or obstructs the Consumer's experience on the Controller's web page or application.

F. Example: A Consumer opts out of the use of Personal Data for Sale or Targeted Advertising using a Universal Opt-Out Mechanism. The Consumer visits a fashion retailer's website. The fashion retailer's homepage contains a message at the top of the webpage that displays the Consumer's opt-out status, stating, "you have opted out of targeted advertising" next to a link that states "Opt-in to Data Use". The linked webpage also meets all requirements of 4 CCR 904-3, Rules 7.03 and 7.04. Consent pursuant to this request is valid.

Rule 7.06 CONSENT FOR CHILDREN

A. When a Controller engages in Processing activities involving the collection and Processing of Personal Data from a known Child or operates a website or business directed to Children or has actual knowledge that it is collecting or maintaining Personal Data from a Child, the Controller must obtain Consent from the parent or lawful guardian of that Child before collecting or Processing the Child's Personal Data.

B. A Controller Processing the Personal Data of a Child must make reasonable efforts to obtain verifiable parental Consent, taking into consideration available technology. Any method to obtain verifiable parental Consent must be reasonably calculated, in light of available technology, to ensure that the person providing Consent is the Child's parent or lawful guardian.

C. Reasonably calculated methods for determining that a person Consenting to the Processing of a Child's Personal Data is the parent or lawful guardian of that Child include, but are not limited to:

1. Providing a Consent form to be signed by the parent or guardian under penalty of perjury and returned to the business by postal mail, facsimile, or electronic scan;

2. Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;

3. Having a parent or guardian call a toll-free telephone number staffed by trained personnel;

4. Having a parent or guardian connect to trained personnel via videoconference; and

5. Verifying a parent or guardian's identity by checking a form of government-issued identification against databases of such information, as long as the parent or guardian's identification is deleted by the business from its records promptly after such verification is complete.

D. Any Personal Data collected for purposes of verifying the identity of a parent or legal guardian may not be used for any reason other than Processing these verifications.

Rule 7.07 REFUSING OR WITHDRAWING CONSENT

A. A Consumer shall be able to refuse or revoke Consent as easily and within a similar number of steps as Consent is affirmatively provided.

B. If Consent is obtained through an electronic interface, the Consumer shall be able to refuse or withdraw Consent through the same or similar electronic interface.

C. When using an electronic interface, and when feasible based on the Consumer's relationship with the Controller, a Controller may allow Consumers to track what Processing activities they have Consented to or opted out of.

D. There shall be no detriment to a Consumer for refusing or withdrawing Consent, consistent with C.R.S. § 6-1-1308(1)(c)(II), and 4 CCR 904-3, Rule 6.05.

1. Notwithstanding 4 CCR 904-3 Rule 7.07(D), if a Consumer refuses to Consent to, or withdraws consent for the Processing of Sensitive Data or Personal Data strictly necessary for a program, product or service, the Controller is no longer obligated to provide that program, product or service.

E. If a Consumer withdraws Consent for a Processing activity, subject to Consent under C.R.S. §§ 6-1-1306(1)(a)(IV)(C), 1308(4), and 1308(7), the Controller shall cease that Processing activity and, in the notice required by C.R.S. § 6-1-1306(2), provide the Consumer instructions on how to exercise the right to deletion, provide a link to exercise the right to deletion, or inform the Consumer that information regarding the right to delete their Personal Data can be found in the Controller's privacy notice.

Rule 7.08 REFRESHING CONSENT

A. When a Consumer has not interacted with a Controller in the prior twenty-four (24) months, the Controller must refresh Consent in compliance with all requirements of this Part 7 to:

1. Continue Processing Sensitive Data pursuant to C.R.S. § 6-1-1308(7); or

2. Continue Processing Personal Data for a Secondary Use pursuant to C.R.S. § 1308(4), if the Secondary Use involves Profiling for a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services.

B. Controllers are not required to refresh Consent under part A of this section where a Consumer has access and ability to update their opt-out preferences at any time through a user-controlled interface.

C. If a Processing purpose materially evolves such that the new purpose becomes a secondary use pursuant to C.R.S. § 6-1-1308(4), the Consumer's original Consent is no longer valid, and the Controller must obtain new Consent pursuant to Part 7 of these rules.

Rule 7.09 USER INTERFACE DESIGN, CHOICE ARCHITECTURE, AND DARK PATTERNS

A. The following principles should be considered when designing a user interface or a choice architecture used to obtain Consent when required under C.R.S. §§ 6-1-1303(5), 6-1- 1306(1)(a)(IV)(C), 6-1-1308(4), and 6-1-1308(7):

1. Consent choice options should be presented to Consumers in a symmetrical way that does not impose unequal weight or focus on one available choice over another such that a Consumer's ability to consent is impaired or subverted.

a. Example: One choice should not be presented with less prominent size, font, or styling than the other choice. Presenting an "I accept" button in a larger size than the "I do not accept" button would not be considered equal or symmetrical. Presenting an "I do not accept" button in a greyed-out color while the "I accept" button is presented in a bright or obvious color would not be considered equal or symmetrical.

b. Example: If multiple choices are offered to a Consumer, it should be equally easy to accept or reject all options. Presenting the option to "accept all" when offering a Consumer the choice to Consent to the use of Sensitive Data for multiple purposes without an option to "reject all" would not be considered equal or symmetrical.

2. Consent choice options should avoid the use of emotionally manipulative language or visuals to unfairly, fraudulently, or deceptively coerce or steer Consumer choice or Consent.

   a. Example: One choice should not be presented in a way that creates unnecessary guilt or shames the user into selecting a specific choice. Presenting the choices "I accept, I want to help endangered species" vs "No, I don't care about animals" may be considered unfairly emotionally manipulative.

   b. Example: The explanation of the choice to Consumers should not include gratuitous information to emotionally manipulate Consumers. Explaining that a mobile application "helps save lives" when asking for Consent to collect Sensitive Data for Targeted Advertising may be considered deceptively emotionally manipulative if the Targeted Advertising is not critical to the lifesaving functionality of the application.

3. A Consumer's silence or failure to take an affirmative action should not be interpreted as acceptance or Consent.

   a. Example: A Consumer closing a pop-up window which requests Consent without first affirmatively selecting the equivalent of an "I accept" button should not be interpreted as Consent.

   b. Example: A Consumer navigating forward on a webpage after a Consent choice has been presented without selecting the equivalent of an "I accept" button should not be interpreted as affirmative Consent.

   c. Example: A Consumer continuing to use a Smart TV without replying "I accept" or "I consent" in reply to a verbal request for Consent should not be interpreted as affirmative Consent.

4. Consent choice options should not be presented with a preselected or default option.

   a. Example: Checkboxes or radio buttons should not be selected automatically when presented to a Consumer.

5. A Consumer should be able to select either Consent choice option within a similar number of steps. A Consumer's ability to exercise a more privacy-protective option shall not be unduly longer, more difficult, or time-consuming than the path to exercise a less privacy-protective option.

   a. Example: Consumers should be presented with all choices at the same time. Presenting an "I accept" button next to a "Learn More" button which requires Consumers to take an extra step before they are given the option of an "I do not accept" button could be considered an unnecessary restriction.

   b. Example: Describing the choice before Consumers and placing both the "I accept" and "I do not accept" buttons after a "select preferences" button would not be considered an unnecessary restriction.

6. A Consumer's expected interaction with a website, application, or product should not be unnecessarily interrupted or intruded upon to request Consent.

   a. Example: Consumers should not be interrupted multiple times in one visit to a website to Consent if they have declined the Consent choice offered when they arrived at the page.

   b. Example: Consumers should not be redirected away from the content or service they are attempting to interact with because they declined the Consent choice offered, unless Consent to process the requested data is strictly necessary to provide the website or application content or experience.

c. Example: Consumers should not be forced to navigate through multiple pop-ups which cover or otherwise disrupt the content or service they are attempting to interact with because they declined the Consent choice offered.

7. Consent choice options should not include misleading statements, omissions, affirmative misstatements, or intentionally confusing language to obtain Consent.

   a. Example: Choices should not be driven by a false sense of urgency. A countdown clock displayed next to a Consent choice option which states "time is running out to Consent to this data use and receive a limited discount" where the discount is not actually limited by time or availability would be considered creating a false sense of urgency.

   b. Example: Choices should avoid the use of double negatives when describing Consent choice options to Consumers.

   c. Example: Consent choice options should not be presented with confusing or unexpected syntax. "Please do not check this box if you wish to Consent to this data use" would be considered confusing syntax.

   d. Example: The language used for choice options should logically follow the question presented to the Consumer. Offering the options of "Yes" or "No" to the question "Do you wish to provide or decline Consent for the described purposes" would be considered an illogical choice option. The choice options "provide" and "decline" would be considered to logically follow the same question.

8. The vulnerabilities or unique characteristics of the target audience of a product, service, or website should be considered when deciding how to present Consent choice options.

   a. Example: A website or service that primarily interacts with Consumers under the age of 18 should consider the simplicity of the language used to explain the choice options or the way in which cartoon imagery or endorsements might unduly influence their choice.

   b. Example: A website or service that primarily interacts with the elderly should consider font size and space between buttons to ensure readability and ease of interaction with design elements.

9. User interface design and Consent choice architecture should operate in a substantially similar manner when accessed through digital accessibility tools.

   a. Example: If it takes two clicks for a Consumer to Consent through a website, it should take no more than two actions for a Consumer using a digital accessibility tool to complete the same Consent process.

B. In addition to the principles included in this part 4 CCR 904-3, Rule 7.09(A), Controllers may consider statutes, administrative rules, and administrative guidance concerning Dark Patterns from other jurisdictions when evaluating the appropriateness of the user interface or choice architecture used to obtain required Consent.

C. Controllers shall not use an interface design or choice architecture to obtain required Consent that has been designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making or choice, or unfairly, fraudulently, or deceptively manipulating or coercing a Consumer into providing Consent.

1. The principles outlined in 4 CCR 904-3, Rule 7.09(A) and (B) are factors to be considered when determining if a consent interface design or choice architecture has been designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making or choice, or unfairly, fraudulently, or deceptively manipulating or coercing a Consumer into providing Consent.

D. Consent obtained in violation of this part 4 CCR 904-3, Rule 7.09(C) may be considered a Dark Pattern, as defined in C.R.S. § 6-1-1303(9).

E. The fact that a design or practice is commonly used is not, alone, enough to demonstrate that any particular design or practice is not a Dark Pattern.

F. Consent obtained through Dark Patterns does not constitute valid Consent in compliance with C.R.S. §§ 6-1-1303, 6-1-1306, and 6-1-1308.

PART 8 DATA PROTECTION ASSESSMENTS

Rule 8.02 SCOPE

A. A data protection assessment shall be a genuine, thoughtful analysis of each Personal Data Processing activity that presents a heightened risk of harm to a Consumer, pursuant to C.R.S. § 6-1-1309(3), that: 1) identifies and describes the risks to the rights of consumers associated with the processing; 2) documents measures considered and taken to address and offset those risks, including those duties required by C.R.S. § 6-1-1308; 3) contemplates the benefits of the Processing; and 4) demonstrates that the benefits of the Processing outweigh the risks offset by safeguards in place.

B. If a Controller conducts a data protection assessment for the purpose of complying with another jurisdiction's law or regulation, the assessment shall satisfy the requirements established in this section if such data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.

1. If a data protection assessment conducted for the purpose of complying with another jurisdiction's law or regulation is not similar in scope and effect to a data protection assessment created pursuant to this section, a Controller may submit that assessment with a supplement that contains any additional information required by this jurisdiction.

C. The depth, level of detail, and scope of data protection assessments should take into account the scope of risk presented, the size of the Controller, amount and sensitivity of Personal Data Processed, Personal Data Processing activities subject to the assessment, and complexity of safeguards applied.

D. A "comparable set of Processing operations" that can be addressed by a single data protection assessment pursuant to C.R.S. § 6-1-1309(5) is a set of similar Processing operations including similar activities that present heightened risks of similar harm to a Consumer.

1. Example: The ACME Toy Store chain is considering using in-store paper forms to collect names, mailing addresses, and birthdays from Children that visit their stores, and using that information to mail a coupon and list of age-appropriate toys to each child during the Child's birth month and every November. ACME uses the same Processors and Processing systems for each category of mailings across all stores. ACME must conduct and document a data protection assessment because it is Processing Personal Data from known Children, which is Sensitive Data. ACME can use the same data protection assessment for Processing the Personal Data for the birthday mailing and November mailing across all stores because in each case it is collecting the same categories of Personal Data in the same way for the purpose of sending coupons and age-appropriate toy lists to Children.

Rule 8.03 STAKEHOLDER INVOLVEMENT

A. A data protection assessment shall involve all relevant internal actors from across the Controller's organizational structure, and where appropriate, relevant external parties, to identify, assess and address the data protection risks.

Rule 8.04 DATA PROTECTION ASSESSMENT CONTENT

A. At a minimum, a data protection assessment must include the following information:

1. A short summary of the Processing activity;

2. The categories of Personal Data to be Processed and whether they include Sensitive Data, including Personal Data from a known Child as described in C.R.S. § 6-1-1303(24);

3. The context of the Processing activity, including the relationship between the Controller and the Consumers whose Personal Data will be Processed, and the reasonable expectations of those Consumers;

4. The nature and operational elements of the Processing activity. In determining the level of detail and specificity to provide pursuant to this section, the Controller shall consider the type, amount, and sensitivity of Personal Data Processed, the impacts that operational elements will have on the level of risk presented by the Processing activity, and any relevant unique relationships. Relevant operational elements may include:

   a. Sources of Personal Data;

   b. Technology or Processors to be used;

   c. Names or categories of Personal Data recipients, including Third Parties, Affiliates, and Processors that will have access to the Personal Data, the processing purpose for which the Personal Data will be provided to those recipients, and categorical compliance processes that the Controller uses to evaluate that type of recipient;

   d. Operational details about the Processing, including planned processes for Personal Data collection, use, storage, retention, and sharing;

   e. Specific types of Personal Data to be processed.

5. The core purposes of the Processing activity, as well as other benefits of the Processing that may flow, directly and indirectly to the Controller, Consumer, other expected stakeholders, and the public;

6. The sources and nature of risks to the rights of Consumers associated with the Processing activity posed by the Processing activity. The source and nature of the risks may differ based on the processing activity and type of Personal Data processed. Risks to the rights of Consumers that a Controller may consider in a data protection assessment include, for example, risks of:

   a. Constitutional harms, such as speech harms or associational harms;

   b. Intellectual privacy harms, such as the creation of negative inferences about an individual based on what an individual reads, learns, or debates;

   c. Data security harms, such as unauthorized access or adversarial use;

   d. Discrimination harms, such as a violation of federal antidiscrimination laws or antidiscrimination laws of any state or political subdivision thereof, or unlawful disparate impact;

   e. Unfair, unconscionable, or deceptive treatment;

   f. A negative outcome or decision with respect to an individual's eligibility for a right, privilege, or benefit related to financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services;

g. Financial injury or economic harm;

h. Physical injury, harassment, or threat to an individual or property;

i. Privacy harms, such as physical or other intrusion upon the solitude or seclusion or the private affairs or concerns of Consumers, stigmatization or reputational injury;

j. Psychological harm, including anxiety, embarrassment, fear, and other mental trauma; or

k. Other detrimental or negative consequences that affect an individual's private life, private affairs, private family matters or similar concerns, including actions and communications within an individual's home or similar physical, online, or digital location, where an individual has a reasonable expectation that Personal Data or other data will not be collected, observed, or used.

7. Measures and safeguards the Controller will employ to reduce the risks identified by the Controller pursuant to 4 CCR 904-3, Rule 8.04(A)(6). Measures shall include the following, as applicable:

a. The use of De-identified Data;

b. Measures taken pursuant to the Controller duties in C.R.S. § 6-1-1308, including an overview of data security practices the Controller has implemented, any data security assessments that have been completed pursuant to C.R.S. § 6-1- 1308(5), and any measures taken to comply with the consent requirements of 4 CCR 904-3, Rule 7; and

c. Measures taken to ensure that Consumers have access to the rights provided in C.R.S. § 6-1-1306.

8. A description of how the benefits of the Processing outweigh the risks identified pursuant to 4 CCR 904-3, Rule 8.04(A)(6), as mitigated by the safeguards identified pursuant to 4 CCR 904-3, Rule 8.04(A)(7).

a. Contractual agreements in place to ensure that Personal Data in the possession of a Processor or other Third Party remains secure; or

b. Any other practices, policies, or trainings intended to mitigate Processing risks.

9. If a Controller is Processing Personal Data for Profiling as contemplated in C.R.S. § 6-1- 1309(2)(a), a data protection assessment of that Processing activity must also comply with 4 CCR 904-3, Rule 9.06;

10. If a Controller is Processing Sensitive Data pursuant to the exception in section 4 CCR 904-3, Rule 6.10, the details of the process implemented to ensure that Personal Data and Sensitive Data Inferences are not transferred and are deleted within twenty-four (24) hours of the Personal Data Processing activity;

11. Relevant internal actors and external parties contributing to the data protection assessment;

12. Any internal or external audit conducted in relation to the data protection assessment, including, the name of the auditor, the names and positions of individuals involved in the review process, and the details of the audit process; and

13. Dates the data protection assessment was reviewed and approved, and names, positions, and signatures of the individuals responsible for the review and approval.

Rule 8.05 TIMING

A. A Controller shall conduct and document a data protection assessment before initiating a Processing activity that Presents a Heightened Risk of Harm to a Consumer, as defined at C.R.S. § 6-1-1309(2).

B. A Controller shall review and update the data protection assessment as often as appropriate considering the type, amount, and sensitivity of Personal Data Processed and level of risk presented by the Processing, throughout the Processing activity's lifecycle in order to: 1) monitor for harm caused by the Processing and adjust safeguards accordingly; and 2) ensure that data protection and privacy are considered as the Controller makes new decisions with respect to the Processing.

C. Data protection assessments containing Processing for Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer shall be reviewed and updated at least annually, and include an updated evaluation for fairness and disparate impact and the results of any such evaluation.

D. A new data Processing activity is generated when existing Processing activities are modified in a way that materially changes the level of risk presented. When a new data Processing activity is generated, a data protection assessment must reflect changes to the pre-existing activity and additional considerations and safeguards to offset the new risk level.

1. Modifications that may materially change the level of risk of a Processing activity may include, without limitation, changes to any of the following:

    a. The way that existing systems or Processes handle Personal Data;

    b. Processing purpose;

    c. Personal data Processed or sources of Personal Data;

    d. Method of collection of Personal Data;

    e. Personal Data recipients;

    f. Processor roles or Processors;

    g. Algorithm applied or algorithmic result; or

    h. Software or other systems used for Processing.

E. Data protection assessments, including prior versions which have been revised when a new data Processing activity is generated, shall be stored for as long as the Processing activity continues, and for at least three (3) years after the conclusion of the Processing activity. Data protection assessments shall be held in an electronic, transferable form.

F. Data protection assessments shall be required for activities created or generated after July 1, 2023. This requirement is not retroactive.

Rule 8.06 ATTORNEY GENERAL REQUESTS

A. A Controller shall make the data protection assessment available to the Attorney General within thirty (30) days of the Attorney General's request.

PART 9 PROFILING

Rule 9.01 AUTHORITY AND PURPOSE

A. The statutory authority for the rules in this Part 9 is C.R.S. §§ 6-1-108(1), 6-1-1302(1)(c)(II)(B), 6- 1-1303, 6-1-1306, 6-1-1309, and 6-1-1313. The purpose of the rules in this Part 9 is to provide clarity on the duties and rights related to Profiling.

Rule 9.02 SCOPE

A. Controllers have an affirmative obligation to provide clear, understandable, and transparent information to Consumers about how their Personal Data is used, including for Profiling, pursuant to C.R.S. § 6-1-1302(1)(c)(II)(B).

B. Consumers have the right to opt out of Profiling as defined in C.R.S. § 6-1-1303(20) and 4 CCR 904-3, Rule 2.02 when the Profiling is done in furtherance of a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services, pursuant to C.R.S. §§ 6-1-1306(1)(a)(I).

C. Controllers must conduct and document a data protection assessment compliant with C.R.S. § 6- 1-1309 and Parts 8 and 9 of these rules before Processing Personal Data for Profiling that presents specific, reasonably foreseeable risks contemplated in C.R.S. § 6-1-1309(2)(a).

Rule 9.03 PROFILING OPT-OUT TRANSPARENCY

A. To ensure that Consumers understand how their Personal Data is used for Profiling in furtherance of Decisions that Produce Legal or Other Similarly Significant Effects Concerning a Consumer, Controllers that Process Personal Data for Profiling for a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services and subject to C.R.S. § 6-1-1306(1)(a)(I) shall provide clear, understandable, and transparent information to Consumers in the required privacy notice, including at a minimum:

1. What decision(s) is (are) subject to Profiling;

2. The categories of Personal Data that were or will be Processed as part of the Profiling in Furtherance of Decisions that Produce Legal or Other Similarly Significant Effects;

3. A non-technical, plain language explanation of the logic used in the Profiling process;

4. A non-technical, plain language explanation of how Profiling is used in the decision- making process, including the role of human involvement, if any;

5. If the system has been evaluated for accuracy, fairness, or bias, including the impact of the use of Sensitive Data, and the outcome of any such evaluation;

6. The benefits and potential consequences of the decision based on the Profiling; and

7. Information about how a Consumer may exercise the right to opt out of the Processing of Personal Data concerning the Consumer for Profiling in Furtherance of Decisions that Produce Legal or Other Similarly Significant Effects.

B. Notwithstanding the requirements in 4 CCR 904-3, Rule 9.03(A), nothing in 4 CCR 904-3, Rule shall be construed as requiring the Controller to provide information to a Consumer in a manner that would disclose the Controller's trade secrets.

Rule 9.04 OPTING OUT OF PROFILING IN FURTHERANCE OF DECISIONS THAT PRODUCE LEGAL OR SIMILARLY SIGNIFICANT EFFECTS CONCERNING A CONSUMER

A. Consumers have the right to opt out of Profiling in furtherance of Decisions that Produce Legal or other Similarly Significant Effects Concerning a Consumer through the method specified by the Controller in the required privacy notice, pursuant to C.R.S. § 6-1-1306(1)(a) and 4 CCR 904-3, Rule 4.03.

B. Requests to opt out of Profiling in furtherance of Decisions that Produce Legal or other Similarly Significant Effects Concerning a Consumer based on Solely Automated Processing or Human Reviewed Automated Processing shall be honored pursuant to C.R.S. § 6-1-1306(2).

C. A Controller may decide not to take action on a request to opt out of Profiling in furtherance of Decisions that Produce Legal or other Similarly Significant Effects Concerning a Consumer if the Profiling used is based on Human Involved Automated Processing. If a Controller does not take action based on this reason, the Controller shall inform the Consumer pursuant to C.R.S. § 6-1- 1306(2)(b) and include the following information, or share a link to such information if it is included in the Controller's privacy notice:

1. The decision subject to the Profiling;

2. The categories of Personal Data that were or will be used as part of the Profiling used in Furtherance of Decisions that Produce Legal or Other Similarly Significant Effects;

3. A non-technical, plain language explanation of the logic used in the Profiling process;

4. A non-technical, plain language explanation of the role of meaningful human involvement in Profiling and the decision-making process;

5. How Profiling is used in the decision-making process;

6. The benefits and potential consequences of the decision based on the Profiling; and

7. An explanation of how Consumers can correct or delete the Personal Data used in the Profiling used in the decision-making process.

D. In order to ensure that Consumers have an opportunity to exercise their right to opt out of Profiling in furtherance of Decisions that Produce Legal or Other Similarly Significant Effects Concerning a Consumer, Controllers that Process Personal Data for Profiling covered by C.R.S. §§ 6-1-1303(10) and 6-1-1306(1)(a)(I) shall provide a method to exercise the right to opt out of Profiling in furtherance of Decision that Produce Legal or Other similarly Significant Effects Concerning a Consumer clearly and conspicuously at or before the time such Processing occurs.

E. Notwithstanding the requirements in 4 CCR 904-3, Rule 9.04(C), nothing in 4 CCR 904-3, Rule shall be construed as requiring the Controller to provide information to a Consumer in a manner that would disclose the Controller's trade secrets.

Rule 9.05 CONSENT FOR PROFILING IN FURTHERANCE OF DECISIONS THAT PRODUCE LEGAL OR SIMILARLY SIGNIFICANT EFFECTS CONCERNING A CONSUMER

A. When a Consumer has opted out of Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer as defined by C.R.S. § 6-1-1303(10), the Controller may request that a Consumer provide Consent after opting out subject to 4 CCR 904- 3, Rule 7.05.

B. If a Controller decides to begin Processing Personal Data for Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer and such Processing is not reasonably necessary to or compatible with the original specified purposes for which the Personal Data was Processed, the Controller shall request the Consumer provide Consent prior to such processing, subject to C.R.S. § 6-1-1308(4) and Part 7 of these rules.

C. Any request for Consent to Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer must include meaningful information about the Profiling that allows a Consumer to make an informed, freely given, and specific choice, including, at a minimum:

1. The decision subject to the Profiling;

2. The categories of Personal Data used in the Profiling;

3. A non-technical, plain language explanation of the logic used in the Profiling, or a link to such information if it is included in the Controller's privacy notice;

4. How Profiling is used in the decision-making process, including the role of human involvement, if any;

5. Why the Profiling is relevant to the decision-making process;

6. Potential benefits and consequences of the decision based on the Profiling; and

7. Any applicable links to where Consumers can find any additional information about the Profiling and decision-making process and their associated rights.

D. Notwithstanding the requirements in 4 CCR 904-3, Rule 9.05(C), nothing in 4 CCR 904-3, Rule shall be constructed as requiring the Controller to provide information to a Consumer in a manner that would disclose the Controller's trade secrets.

Rule 9.06 DATA PROTECTION ASSESSMENTS FOR PROFILING

A. Controllers must conduct and document a data protection assessment compliant with C.R.S. § 6- 1-1309 and 4 CCR 904-3, Part 8 before Processing Personal Data for Profiling if the Profiling presents a reasonably foreseeable risk of:

1. Unfair or deceptive treatment of, or unlawful disparate impact on Consumers;

2. Financial or physical injury to Consumers;

3. A physical or other intrusion upon the solitude or seclusion, or private affairs or concerns, of Consumers if the intrusion would be offensive to a reasonable person; or

4. Other substantial injury to Consumers.

B. Profiling under C.R.S. § 6-1-1309(2)(a) and covered by required data protection assessment obligations includes Profiling using Solely Automated Processing, Human Reviewed Automated Processing, and Human Involved Automated Processing.

C. "Unfair or deceptive treatment" as used in C.R.S. § 6-1-1309 and 4 CCR 904-3, Rule 9.06 includes conduct or activity which violates state or federal laws that prohibit unfair and deceptive commercial practices.

D. "Unlawful disparate impact" as used in C.R.S. § 6-1-1309 and 4 CCR 904-3, Rule 9.06 includes conduct or activity which violates state or federal laws that prohibit unlawful discrimination against Consumers.

E. Controllers should consider both the type and degree of potential harm to Consumers when determining if Profiling presents a reasonably foreseeable risk of "other substantial injury" to Consumers as used in C.R.S. § 6-1-1309 and 4 CCR 904-3, Rule 9.06(A). For example, a small harm to a large number of Consumers. may constitute "other substantial injury".

F. If a Controller is Processing Personal Data for Profiling under C.R.S. § 6-1-1309(2)(a), a data protection assessment of that Processing activity must include the elements listed at 4 CCR 904- 3, Rule 8.04 as well as each of the following as applicable to the assessed reasonably foreseeable risk:

1. The specific types of Personal Data that were or will be used in the Profiling or decision- making process;

2. The decision to be made using Profiling;

3. The benefits of automated processing over manual processing for the stated purpose;

4. A plain language explanation of why the Profiling directly and reasonably relates to the Controller's goods and services;

5. An explanation of the training data and logic used to create the Profiling system, including any statistics used in the analysis, either created by the Controller or provided by a Third Party which created the applicable Profiling system or software;

6. If the Profiling is conducted by Third Party software purchased by the Controller, the name of the software and copies of any internal or external evaluations sufficient to show of the accuracy and reliability of the software where relevant to the risks described in C.R.S. § 6-1-1309(2)(a)(I)-(IV);

7. A plain language description of the outputs secured from the Profiling process;

8. A plain language description of how the outputs from the Profiling process are or will be used, including whether and how they are used to make a decision to provide or deny or substantially contribute to the provision or denial of financial or lending services, housing, insurance, education, enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services;

9. If there is human involvement in the Profiling process, the degree and details of any human involvement;

10. How the Profiling system is evaluated for fairness and disparate impact, and the results of any such evaluation;

11. Safeguards used to reduce the risk of harms identified; and

12. Safeguards for any data sets produced by or derived from the Profiling.

G. If a Controller conducts a data protection assessment which includes an assessment of relevant Profiling for the purpose of complying with another jurisdiction's law or regulation, the assessment shall satisfy the requirements established in this section if such data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section. A Controller may also submit an assessment with a supplement that contains any additional information required by this regulation.

PART 10 ENFORCEMENT

Rule 10.01 AUTHORITY AND PURPOSE

A. The statutory authority for the rules in this Part 10 is C.R.S. §§ 6-1-1310 and 6-1-1311. The purpose of the rules in this Part 10 is to clarify enforcement considerations related to the Colorado Privacy Act, C.R.S. § 6-1-1303, et seq., and these Colorado Privacy Act Rules, 4 CCR 904-3. Rule

Rule 10.02 ENFORCEMENT CONSIDERATIONS

A. Nothing in the Colorado Privacy Act, C.R.S. § 6-1-1303, et seq., or these Colorado Privacy Act Rules, 4 CCR 904-3, provides the Colorado Attorney General or District Attorney, as applicable, with enforcement powers that would infringe upon rights protected by the United States Constitution or Colorado Constitution, including the right to freedom of speech or freedom of the press.

PART 11 MATERIALS INCORPORATED BY REFERENCE

Rule 11.01 AUTHORITY AND PURPOSE

A. The statutory authority for the rules in this Part 10 is C.R.S. §§ 6-1-108(1) and 6-1-1313. The purpose of the rules in this Part 11 is to incorporate by reference the guidelines that are referred to in 4 CCR 904-3, Rule 3.02(A)(2).

Rule 11.02 WEB CONTENT ACCESSIBILITY GUIDELINES

A. The Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, are hereby incorporated into 4 CCR 904-3, Rule 3.02(A)(2) by reference pursuant to C.R.S. § 24-4-103(12.5), and do not include any later amendments.

B. Copies of the Web Content Accessibility Guidelines that are incorporated by reference into these rules may be obtained by sending a written request to the following address by U.S. mail: Colorado Department of Law Ralph L. Carr Judicial Center 1300 Broadway, 9th Floor Denver, CO 80203.

C. The Web Content Accessibility Guidelines published by the World Wide Web Consortium incorporated by reference into these rules are available at no cost in an electronic form online at https://www.w3.org/TR/WCAG21/.

D. The Colorado Department of Law also maintains a copy of the Web Content Accessibility Guidelines that are incorporated by reference into these rules that is available for public inspection at the Colorado Department of Law's office during regular business hours.

Connecticut Consumer Data Privacy and Online Monitoring

Sec. 42-515. (Note: This section is effective July 1, 2023.) Definitions.

As used in this section and sections 42-516 to 42-525, inclusive, unless the context otherwise requires:

(1) "Affiliate" means a legal entity that shares common branding with another legal entity or controls, is controlled by or is under common control with another legal entity. For the purposes of this subdivision, "control" or "controlled" means (A) ownership of, or the power to vote, more than fifty per cent of the outstanding shares of any class of voting security of a company, (B) control in any manner over the election of a majority of the directors or of individuals exercising similar functions, or (C) the power to exercise controlling influence over the management of a company.

(2) "Authenticate" means to use reasonable means to determine that a request to exercise any of the rights afforded under subdivisions (1) to (4), inclusive, of subsection (a) of section 42-518 is being made by, or on behalf of, the consumer who is entitled to exercise such consumer rights with respect to the personal data at issue.

(3) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include (A) a digital or physical photograph, (B) an audio or video recording, or (C) any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

(4) "Business associate" has the same meaning as provided in HIPAA.

(5) "Child" has the same meaning as provided in COPPA.

(6) "Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the consumer. "Consent" may include a written statement, including by electronic means, or any other unambiguous affirmative action. "Consent" does not include (A) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information, (B) hovering over, muting, pausing or closing a given piece of content, or (C) agreement obtained through the use of dark patterns.

(7) "Consumer" means an individual who is a resident of this state. "Consumer" does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit or government agency.

(8) "Controller" means an individual who, or legal entity that, alone or jointly with others determines the purpose and means of processing personal data.

(9) "COPPA" means the Children's Online Privacy Protection Act of 1998, 15 USC 6501 et seq., and the regulations, rules, guidance and exemptions adopted pursuant to said act, as said act and such regulations, rules, guidance and exemptions may be amended from time to time.

(10) "Covered entity" has the same meaning as provided in HIPAA.

(11) "Dark pattern" (A) means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, and (B) includes, but is not limited to, any practice the Federal Trade Commission refers to as a "dark pattern".

(12) "Decisions that produce legal or similarly significant effects concerning the consumer" means decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services.

(13) "De-identified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the controller that possesses such data (A) takes reasonable measures to ensure that such data cannot be associated with an individual, (B) publicly commits to process such data only in a de-identified fashion and not attempt to re-identify such data, and (C) contractually obligates any recipients of such data to satisfy the criteria set forth in subparagraphs (A) and (B) of this subdivision.

(14) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et seq., as amended from time to time.

(15) "Identified or identifiable individual" means an individual who can be readily identified, directly or indirectly.

(16) "Institution of higher education" means any individual who, or school, board, association, limited liability company or corporation that, is licensed or accredited to offer one or more programs of higher learning leading to one or more degrees.

(17) "Nonprofit organization" means any organization that is exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the Internal Revenue Code of 1986, or any subsequent corresponding internal revenue code of the United States, as amended from time to time.

(18) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable individual. "Personal data" does not include de-identified data or publicly available information.

(19) "Precise geolocation data" means information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of one thousand seven hundred fifty feet. "Precise geolocation data" does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(20) "Process" or "processing" means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion or modification of personal data.

(21) "Processor" means an individual who, or legal entity that, processes personal data on behalf of a controller.

(22) "Profiling" means any form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

(23) "Protected health information" has the same meaning as provided in HIPAA.

(24) "Pseudonymous data" means personal data that cannot be attributed to a specific individual without the use of additional information, provided such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

(25) "Publicly available information" means information that (A) is lawfully made available through federal, state or municipal government records or widely distributed media, and (B) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public.

(26) "Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party. "Sale of personal data" does not include (A) the disclosure of personal data to a processor that processes the personal data on behalf of the controller, (B) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer, (C) the disclosure or transfer of personal data to an affiliate of the controller, (D) the disclosure of personal data where the consumer directs the controller to disclose the personal data

or intentionally uses the controller to interact with a third party, (E) the disclosure of personal data that the consumer (i) intentionally made available to the general public via a channel of mass media, and (ii) did not restrict to a specific audience, or (F) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction, or a proposed merger, acquisition, bankruptcy or other transaction, in which the third party assumes control of all or part of the controller's assets.

(27) "Sensitive data" means personal data that includes (A) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status, (B) the processing of genetic or biometric data for the purpose of uniquely identifying an individual, (C) personal data collected from a known child, or (D) precise geolocation data.

(28) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated Internet web sites or online applications to predict such consumer's preferences or interests. "Targeted advertising" does not include (A) advertisements based on activities within a controller's own Internet web sites or online applications, (B) advertisements based on the context of a consumer's current search query, visit to an Internet web site or online application, (C) advertisements directed to a consumer in response to the consumer's request for information or feedback, or (D) processing personal data solely to measure or report advertising frequency, performance or reach.

(29) "Third party" means an individual or legal entity, such as a public authority, agency or body, other than the consumer, controller or processor or an affiliate of the processor or the controller.

(30) "Trade secret" has the same meaning as provided in section 35-51.

(P.A. 22-15, S. 1.)

History: P.A. 22-15 effective July 1, 2023.

Sec. 42-516. (Note: This section is effective July 1, 2023.) Applicability.

The provisions of sections 42-515 to 42-525, inclusive, apply to persons that conduct business in this state or persons that produce products or services that are targeted to residents of this state and that during the preceding calendar year:

(1) Controlled or processed the personal data of not less than one hundred thousand consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or

(2) controlled or processed the personal data of not less than twenty-five thousand consumers and derived more than twenty-five per cent of their gross revenue from the sale of personal data.

(P.A. 22-15, S. 2.)

History: P.A. 22-15 effective July 1, 2023.

Sec. 42-517. (Note: This section is effective July 1, 2023.) Exemptions.

(a) The provisions of sections 42-515 to 42-525, inclusive, do not apply to any:

(1) Body, authority, board, bureau, commission, district or agency of this state or of any political subdivision of this state;

(2) nonprofit organization;

(3) institution of higher education;

(4) national securities association that is registered under 15 USC 78o-3 of the Securities Exchange Act of 1934, as amended from time to time;

(5) financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq.; or

(6) covered entity or business associate, as defined in 45 CFR 160.103.

(b) The following information and data is exempt from the provisions of sections 42-515 to 42-525, inclusive:

(1) Protected health information under HIPAA;

(2) patient-identifying information for purposes of 42 USC 290dd-2;

(3) identifiable private information for purposes of the federal policy for the protection of human subjects under 45 CFR 46;

(4) identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use;

(5) the protection of human subjects under 21 CFR Parts 6, 50 and 56, or personal data used or shared in research, as defined in 45 CFR 164.501, that is conducted in accordance with the standards set forth in this subdivision and subdivisions (3) and (4) of this subsection, or other research conducted in accordance with applicable law;

(6) information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 USC 11101 et seq.;

(7) patient safety work product for purposes of section 19a-127o and the Patient Safety and Quality Improvement Act, 42 USC 299b-21 et seq., as amended from time to time;

(8) information derived from any of the health care related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA;

(9) information originating from and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this subsection that is maintained by a covered entity or business associate, program or qualified service organization, as specified in 42 USC 290dd-2, as amended from time to time;

(10) information used for public health activities and purposes as authorized by HIPAA, community health activities and population health activities;

(11) the collection, maintenance, disclosure, sale, communication or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by a consumer reporting agency, furnisher or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the Fair Credit Reporting Act, 15 USC 1681 et seq., as amended from time to time;

(12) personal data collected, processed, sold or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 USC 2721 et seq., as amended from time to time;

(13) personal data regulated by the Family Educational Rights and Privacy Act, 20 USC 1232g et seq., as amended from time to time;

(14) personal data collected, processed, sold or disclosed in compliance with the Farm Credit Act, 12 USC 2001 et seq., as amended from time to time;

(15) data processed or maintained (A) in the course of an individual applying to, employed by or acting as an agent or independent contractor of a controller, processor or third party, to the extent that the data is collected and used within the context of that role, (B) as the emergency contact information of an individual under sections 42-515 to 42-525, inclusive, used for emergency contact purposes, or (C) that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under subdivision (1) of this subsection and used for the purposes of administering such benefits; and

(16) personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are used in the Airline Deregulation Act, 49 USC 40101 et seq., as amended from time to time, by an air carrier subject to said act, to the extent sections 42-515 to 42-525, inclusive, are preempted by the Airline Deregulation Act, 49 USC 41713, as amended from time to time.

(c) Controllers and processors that comply with the verifiable parental consent requirements of COPPA shall be deemed compliant with any obligation to obtain parental consent pursuant to sections 42-515 to 42-525, inclusive.

(P.A. 22-15, S. 3.)

History: P.A. 22-15 effective July 1, 2023.

Sec. 42-518. (Note: This section is effective July 1, 2023.) Consumers' rights. Compliance by Controllers. Appeals.

(a) A consumer shall have the right to:

(1) Confirm whether or not a controller is processing the consumer's personal data and access such personal data, unless such confirmation or access would require the controller to reveal a trade secret;

(2) correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;

(3) delete personal data provided by, or obtained about, the consumer;

(4) obtain a copy of the consumer's personal data processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means, provided such controller shall not be required to reveal any trade secret; and

(5) opt out of the processing of the personal data for purposes of (A) targeted advertising, (B) the sale of personal data, except as provided in subsection (b) of section 42-520, or (C) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

(b) A consumer may exercise rights under this section by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice. A consumer may designate an authorized agent in accordance with section 42-519 to exercise the rights of such consumer to opt out of the processing of such consumer's personal data for purposes of subdivision (5) of subsection (a) of this section on behalf of the consumer. In the case of processing personal data of a known child, the parent or legal guardian may exercise such consumer rights on the child's behalf. In the

case of processing personal data concerning a consumer subject to a guardianship, conservatorship or other protective arrangement, the guardian or the conservator of the consumer may exercise such rights on the consumer's behalf.

(c) Except as otherwise provided in sections 42-515 to 42-525, inclusive, a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to said sections as follows:

(1) A controller shall respond to the consumer without undue delay, but not later than forty-five days after receipt of the request. The controller may extend the response period by forty-five additional days when reasonably necessary, considering the complexity and number of the consumer's requests, provided the controller informs the consumer of any such extension within the initial forty-five-day response period and of the reason for the extension.

(2) If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than forty-five days after receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision.

(3) Information provided in response to a consumer request shall be provided by a controller, free of charge, once per consumer during any twelve-month period. If requests from a consumer are manifestly unfounded, excessive or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive or repetitive nature of the request.

(4) If a controller is unable to authenticate a request to exercise any of the rights afforded under subdivisions (1) to (4), inclusive, of subsection (a) of this section using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action pursuant to this section and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise such right or rights until such consumer provides additional information reasonably necessary to authenticate such consumer and such consumer's request to exercise such right or rights. A controller shall not be required to authenticate an opt-out request, but a controller may deny an opt-out request if the controller has a good faith, reasonable and documented belief that such request is fraudulent. If a controller denies an opt-out request because the controller believes such request is fraudulent, the controller shall send a notice to the person who made such request disclosing that such controller believes such request is fraudulent, why such controller believes such request is fraudulent and that such controller shall not comply with such request.

(5) A controller that has obtained personal data about a consumer from a source other than the consumer shall be deemed in compliance with a consumer's request to delete such data pursuant to subdivision (3) of subsection (a) of this section by (A) retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the controller's records and not using such retained data for any other purpose pursuant to the provisions of sections 42-515 to 42-525, inclusive, or (B) opting the consumer out of the processing of such personal data for any purpose except for those exempted pursuant to the provisions of sections 42-515 to 42-525, inclusive.

(d) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Not later than sixty days after receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint.

(P.A. 22-15, S. 4.)

History: P.A. 22-15 effective July 1, 2023.

Sec. 42-519. (Note: This section is effective July 1, 2023.) Authorized agents and consumer opt-out.

A consumer may designate another person to serve as the consumer's authorized agent, and act on such consumer's behalf, to opt out of the processing of such consumer's personal data for one or more of the purposes specified in subdivision (5) of subsection (a) of section 42-518. The consumer may designate such authorized agent by way of, among other things, a technology, including, but not limited to, an Internet link or a browser setting, browser extension or global device setting, indicating such consumer's intent to opt out of such processing. A controller shall comply with an opt-out request received from an authorized agent if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on such consumer's behalf.

(P.A. 22-15, S. 5.)

History: P.A. 22-15 effective July 1, 2023.

Sec. 42-520. (Note: This section is effective July 1, 2023.) Controllers' duties. Sale of personal data to third parties. Notice and disclosure to consumers. Consumer opt-out.

(a) A controller shall:

(1) Limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer;

(2) except as otherwise provided in sections 42-515 to 42-525, inclusive, not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;

(3) establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of the personal data at issue;

(4) not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with COPPA;

(5) not process personal data in violation of the laws of this state and federal laws that prohibit unlawful discrimination against consumers;

(6) provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, upon revocation of such consent, cease to process the data as soon as practicable, but not later than fifteen days after the receipt of such request; and

(7) not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data without the consumer's consent, under circumstances where a controller has actual knowledge, and wilfully disregards, that the consumer is at least thirteen years of age but younger than sixteen years of age. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in sections 42-515 to 42-525, inclusive, including denying goods or services, charging different prices or rates for goods or services or providing a different level of quality of goods or services to the consumer.

(b) Nothing in subsection (a) of this section shall be construed to require a controller to provide a product or service that requires the personal data of a consumer which the controller does not collect or maintain, or prohibit a controller from offering a different price, rate, level, quality or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts or club card program.

(c) A controller shall provide consumers with a reasonably accessible, clear and meaningful privacy notice that includes:

(1) The categories of personal data processed by the controller;

(2) the purpose for processing personal data;

(3) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request;

(4) the categories of personal data that the controller shares with third parties, if any;

(5) the categories of third parties, if any, with which the controller shares personal data; and (6) an active electronic mail address or other online mechanism that the consumer may use to contact the controller.

(d) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing.

(e) (1) A controller shall establish, and shall describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights pursuant to sections 42-515 to 42-525, inclusive. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests and the ability of the controller to verify the identity of the consumer making the request. A controller shall not require a consumer to create a new account in order to exercise consumer rights, but may require a consumer to use an existing account. Any such means shall include:

(A) (i) Providing a clear and conspicuous link on the controller's Internet web site to an Internet web page that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising or sale of the consumer's personal data; and

(ii) Not later than January 1, 2025, allowing a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data, through an opt-out preference signal sent, with such consumer's consent, by a platform, technology or mechanism to the controller indicating such consumer's intent to opt out of any such processing or sale. Such platform, technology or mechanism shall:

(I) Not unfairly disadvantage another controller;

(II) Not make use of a default setting, but, rather, require the consumer to make an affirmative, freely given and unambiguous choice to opt out of any processing of such consumer's personal data pursuant to sections 42-515 to 42-525, inclusive;

(III) Be consumer-friendly and easy to use by the average consumer;

(IV) Be as consistent as possible with any other similar platform, technology or mechanism required by any federal or state law or regulation; and

(V) Enable the controller to accurately determine whether the consumer is a resident of this state and whether the consumer has made a legitimate request to opt out of any sale of such consumer's personal data or targeted advertising.

(B) If a consumer's decision to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data, through an opt-out preference signal sent in accordance with the provisions of subparagraph (A) of this subdivision conflicts with the consumer's existing controller-specific privacy setting or voluntary participation in a controller's bona fide loyalty, rewards, premium features, discounts or club

card program, the controller shall comply with such consumer's opt-out preference signal but may notify such consumer of such conflict and provide to such consumer the choice to confirm such controller-specific privacy setting or participation in such program.

(2) If a controller responds to consumer opt-out requests received pursuant to subparagraph (A) of subdivision (1) of this subsection by informing the consumer of a charge for the use of any product or service, the controller shall present the terms of any financial incentive offered pursuant to subsection (b) of this section for the retention, use, sale or sharing of the consumer's personal data.

(P.A. 22-15, S. 6.)

History: P.A. 22-15 effective July 1, 2023.

Sec. 42-521. (Note: This section is effective July 1, 2023.) Processors' duties. Contracts between controllers and processors.

(a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under sections 42-515 to 42-525, inclusive. Such assistance shall include:

(1) Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests;

(2) taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security, as defined in section 36a-701b, of the system of the processor, in order to meet the controller's obligations; and

(3) providing necessary information to enable the controller to conduct and document data protection assessments.

(b) A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties. The contract shall also require that the processor:

(1) Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

(2) at the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

(3) upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in sections 42-515 to 42-525, inclusive;

(4) after providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data; and

(5) allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under sections 42-515 to 42-525, inclusive, using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request.

(c) Nothing in this section shall be construed to relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of such controller's or processor's role in the processing relationship, as described in sections 42-515 to 42-525, inclusive.

(d) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A person who is not limited in such person's processing of personal data pursuant to a controller's instructions, or who fails to adhere to such instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to such processing and may be subject to an enforcement action under section 42-525.

(P.A. 22-15, S. 7.)

History: P.A. 22-15 effective July 1, 2023.

Sec. 42-522. (Note: This section is effective July 1, 2023.) Controllers' data protection assessments. Disclosure to Attorney General.

(a) A controller shall conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer. For the purposes of this section, processing that presents a heightened risk of harm to a consumer includes:

(1) The processing of personal data for the purposes of targeted advertising;

(2) the sale of personal data;

(3) the processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of

(A) unfair or deceptive treatment of, or unlawful disparate impact on, consumers,

(B) financial, physical or reputational injury to consumers,

(C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person, or

(D) other substantial injury to consumers; and (4) the processing of sensitive data.

(b) Data protection assessments conducted pursuant to subsection (a) of this section shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The controller shall factor into any such data protection assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

(c) The Attorney General may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in sections 42-515 to 42-525, inclusive. Data protection assessments shall be confidential and shall be exempt from disclosure under the Freedom of Information Act, as defined in section 1-200. To the extent any information contained in

a data protection assessment disclosed to the Attorney General includes information subject to attorney-client privilege or work product protection, such disclosure shall not constitute a waiver of such privilege or protection.

(d) A single data protection assessment may address a comparable set of processing operations that include similar activities.

(e) If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment shall be deemed to satisfy the requirements established in this section if such data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.

(f) Data protection assessment requirements shall apply to processing activities created or generated after July 1, 2023, and are not retroactive.

(P.A. 22-15, S. 8.)

History: P.A. 22-15 effective July 1, 2023.

Sec. 42-523. (Note: This section is effective July 1, 2023.) De-identified and pseudonymous data. Controllers' duties. Exceptions. Applicability of consumers' rights. Disclosure and oversight.

(a) Any controller in possession of de-identified data shall:

(1) Take reasonable measures to ensure that the data cannot be associated with an individual;

(2) publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and

(3) contractually obligate any recipients of the de-identified data to comply with all provisions of sections 42-515 to 42-525, inclusive.

(b) Nothing in sections 42-515 to 42-525, inclusive, shall be construed to:

(1) Require a controller or processor to re-identify de-identified data or pseudonymous data; or

(2) maintain data in identifiable form, or collect, obtain, retain or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data.

(c) Nothing in sections 42-515 to 42-525, inclusive, shall be construed to require a controller or processor to comply with an authenticated consumer rights request if the controller:

(1) Is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data;

(2) does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer; and

(3) does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.

(d) The rights afforded under subdivisions (1) to (4), inclusive, of subsection (a) of section 42-518 shall not apply to pseudonymous data in cases where the controller is able to demonstrate that any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.

(e) A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

(P.A. 22-15, S. 9.)

History: P.A. 22-15 effective July 1, 2023.

Sec. 42-524. (Note: This section is effective July 1, 2023.) Construction of controllers' and processors' duties.

(a) Nothing in sections 42-515 to 42-525, inclusive, shall be construed to restrict a controller's or processor's ability to:

(1) Comply with federal, state or municipal ordinances or regulations;

(2) comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state, municipal or other governmental authorities;

(3) cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state or municipal ordinances or regulations;

(4) investigate, establish, exercise, prepare for or defend legal claims;

(5) provide a product or service specifically requested by a consumer;

(6) perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty;

(7) take steps at the request of a consumer prior to entering into a contract;

(8) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual, and where the processing cannot be manifestly based on another legal basis;

(9) prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action;

(10) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored and governed by an institutional review board that determines, or similar independent oversight entities that determine, (A) whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller, (B) the expected benefits of the research outweigh the privacy risks, and (C) whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification;

(11) assist another controller, processor or third party with any of the obligations under sections 42-515 to 42-525, inclusive; or

(12) process personal data for reasons of public interest in the area of public health, community health or population health, but solely to the extent that such processing is (A) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed, and (B) under the responsibility of a professional subject to confidentiality obligations under federal, state or local law.

(b) The obligations imposed on controllers or processors under sections 42-515 to 42-525, inclusive, shall not restrict a controller's or processor's ability to collect, use or retain data for internal use to:

(1) Conduct internal research to develop, improve or repair products, services or technology;

(2) effectuate a product recall;

(3) identify and repair technical errors that impair existing or intended functionality; or

(4) perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller, or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

(c) The obligations imposed on controllers or processors under sections 42-515 to 42-525, inclusive, shall not apply where compliance by the controller or processor with said sections would violate an evidentiary privilege under the laws of this state. Nothing in sections 42-515 to 42-525, inclusive, shall be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of the state as part of a privileged communication.

(d) A controller or processor that discloses personal data to a processor or third-party controller in accordance with sections 42-515 to 42-525, inclusive, shall not be deemed to have violated said sections if the processor or third-party controller that receives and processes such personal data violates said sections, provided, at the time the disclosing controller or processor disclosed such personal data, the disclosing controller or processor did not have actual knowledge that the receiving processor or third-party controller would violate said sections. A third-party controller or processor receiving personal data from a controller or processor in compliance with sections 42-515 to 42-525, inclusive, is likewise not in violation of said sections for the transgressions of the controller or processor from which such third-party controller or processor receives such personal data.

(e) Nothing in sections 42-515 to 42-525, inclusive, shall be construed to:

(1) Impose any obligation on a controller or processor that adversely affects the rights or freedoms of any person, including, but not limited to, the rights of any person (A) to freedom of speech or freedom of the press guaranteed in the First Amendment to the United States Constitution, or (B) under section 52-146t; or

(2) apply to any person's processing of personal data in the course of such person's purely personal or household activities.

(f) Personal data processed by a controller pursuant to this section may be processed to the extent that such processing is:

(1) Reasonably necessary and proportionate to the purposes listed in this section; and

(2) adequate, relevant and limited to what is necessary in relation to the specific purposes listed in this section. Personal data collected, used or retained pursuant to subsection (b) of this section shall, where applicable, take into account the nature and purpose or purposes of such collection, use or retention. Such data shall be subject to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to such collection, use or retention of personal data.

(g) If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in subsection (f) of this section.

(h) Processing personal data for the purposes expressly identified in this section shall not solely make a legal entity a controller with respect to such processing.

(P.A. 22-15, S. 10.)

History: P.A. 22-15 effective July 1, 2023.

Sec. 42-525. (Note: This section is effective July 1, 2023.) Enforcement by Attorney General. Notice of violation. Cure period. Report. Penalty.

(a) The Attorney General shall have exclusive authority to enforce violations of sections 42-515 to 42-524, inclusive.

(b) During the period beginning on July 1, 2023, and ending on December 31, 2024, the Attorney General shall, prior to initiating any action for a violation of any provision of sections 42-515 to 42-524, inclusive, issue a notice of violation to the controller if the Attorney General determines that a cure is possible. If the controller fails to cure such violation within sixty days of receipt of the notice of violation, the Attorney General may bring an action pursuant to this section. Not later than February 1, 2024, the Attorney General shall submit a report, in accordance with section 11-4a, to the joint standing committee of the General Assembly having cognizance of matters relating to general law disclosing:

(1) The number of notices of violation the Attorney General has issued;

(2) the nature of each violation;

(3) the number of violations that were cured during the sixty-day cure period; and

(4) any other matter the Attorney General deems relevant for the purposes of such report.

(c) Beginning on January 1, 2025, the Attorney General may, in determining whether to grant a controller or processor the opportunity to cure an alleged violation described in subsection (b) of this section, consider:

(1) The number of violations;

(2) the size and complexity of the controller or processor;

(3) the nature and extent of the controller's or processor's processing activities;

(4) the substantial likelihood of injury to the public;

(5) the safety of persons or property; and (6) whether such alleged violation was likely caused by human or technical error.

(d) Nothing in sections 42-515 to 42-524, inclusive, shall be construed as providing the basis for, or be subject to, a private right of action for violations of said sections or any other law.

(e) A violation of the requirements of sections 42-515 to 42-524, inclusive, shall constitute an unfair trade practice for purposes of section 42-110b and shall be enforced solely by the Attorney General, provided the provisions of section 42-110g shall not apply to such violation.

(P.A. 22-15, S. 11.)

History: P.A. 22-15 effective July 1, 2023.

Secs. 42-526 to 42-530. Reserved for future use.

Delaware Personal Data Privacy Act

Section 1. Amend Title 6 of the Delaware Code by making deletions as shown by strike through and insertions as shown by underline as follows:

Chapter 12D. Delaware Personal Data Privacy Act.

§ 12D-101. Short title.

This chapter shall be known and may be cited as the "Delaware Personal Data Privacy Act."

§ 12D-102. Definitions.

For purposes of this chapter, the following definitions shall apply:

(1) "Affiliate" means a legal entity that shares common branding with another legal entity or controls, is controlled by, or is under common control with another legal entity. For the purposes of this paragraph, "control" or "controlled" means any of the following:

a. Ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting security of a legal entity.

b. Control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

c. The power to exercise controlling influence over the management of a legal entity.

(2) "Authenticate" means to use reasonable means to determine that a request to exercise any of the rights afforded under paragraphs (1) to (4), inclusive, of subsection (a) of § 12D-104 of this chapter is being made by, or on behalf of, the consumer who is entitled to exercise such consumer rights with respect to the personal data at issue.

(3) "Biometric data" means data generated by automatic measurements of an individual's unique biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include any of the following:

a. A digital or physical photograph.

b. An audio or video recording.

c. Any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

(4) "Business associate" means as defined in HIPAA.

(5) "Child" means as defined in COPPA.

(6) "Child abuse" means, with respect to an individual under 18 years of age, as defined in § 901(a) of Title 10, or any equivalent provision in the laws of any other state, the United States, any territory, district, or subdivision of the United States, or any foreign jurisdiction.

(7) "Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the consumer. "Consent" may include a written statement, including by electronic means, or any other unambiguous affirmative action. "Consent" does not include any of the following:

a. Acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information.

b. Hovering over, muting, pausing, or closing a given piece of content.

c. Agreement obtained through the use of dark patterns.

(8) "Consumer" means an individual who is a resident of this State. "Consumer" does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit organization, or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit organization, or government agency.

(9) "Controller" means a person that, alone or jointly with others, determines the purpose and means of processing personal data.

(10) "COPPA" means the Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501, et seq., and the regulations, rules, guidance, and exemptions adopted pursuant to said act, as said act and such regulations, rules, guidance, and exemptions may be amended.

(11) "Covered entity" means as defined in HIPAA.

(12) "Dark pattern" means any of the following:

a. A user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice.

b. Any other practice the Federal Trade Commission refers to as a dark pattern.

(13) "Decisions that produce legal or similarly significant effects concerning the consumer" means decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods or services.

(14) "De-identified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the controller that possesses such data does all of the following:

a. Takes reasonable measures to ensure that such data cannot be associated with an individual.

b. Publicly commits to process such data only in a de-identified fashion and not attempt to re-identify such data.

c. Contractually obligates any recipients of such data to comply with all of the provisions of this chapter applicable to the controller with respect to such data.

(15) "Domestic violence" means as defined in § 1041 of Title 10, or any equivalent provision in the laws of any other state, the United States, any territory, district, or subdivision of the United States, or any foreign jurisdiction.

(16) "Genetic data" means any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. For purposes of this paragraph, "genetic material" includes deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom.

(17) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d, et seq., as amended.

(18) "Human trafficking" means the offense defined in § 787 of Title 11, or any equivalent provision in the laws of any other state, the United States, any territory, district, or subdivision of the United States, or any foreign jurisdiction.

(19) "Identified or identifiable individual" means an individual who can be readily identified, directly or indirectly.

(20) "Nonprofit organization" means any organization that is exempt from taxation under §§ 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the Internal Revenue Code of 1986, or any subsequent corresponding internal revenue code of the United States, as amended.

(21) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable individual, and does not include de-identified data or publicly available information.

(22) "Precise geolocation data" means information derived from technology, including global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet. "Precise geolocation data" does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(23) "Process" or "processing" means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(24) "Processor" means a person that processes personal data on behalf of a controller.

(25) "Profiling" means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, demographic characteristics, personal preferences, interests, reliability, behavior, location, or movements.

(26) "Protected health information" means as defined in HIPAA.

(27) "Pseudonymous data" means personal data that cannot be attributed to a specific individual without the use of additional information, provided such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

(28) "Publicly available information" means any of the following:

a. Information that is lawfully made available through federal, state, or local government records.

b. Information that a controller has a reasonable basis to believe that the consumer has lawfully made available to the general public through widely distributed media.

(29) "Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party. "Sale of personal data" does not include any of the following:

a. The disclosure of personal data to a processor that processes the personal data on behalf of the controller where limited to the purpose of such processing.

b. The disclosure of personal data to a third party for purposes of providing a product or service affirmatively requested by the consumer.

c. The disclosure or transfer of personal data to an affiliate of the controller.

d. The disclosure of personal data where the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party.

e. The disclosure of personal data that the consumer intentionally made available to the general public via a channel of mass media, and did not restrict to a specific audience.

f. The disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other similar transaction in which the third party assumes control of all or part of the controller's assets, or a proposed merger, acquisition, bankruptcy, or other similar transaction in which the third party assumes control of all or part of the controller's assets.

(30) "Sensitive data" means personal data that includes any of the following:

a. Data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis (including pregnancy), sex life, sexual orientation, status as transgender or nonbinary, citizenship status, or immigration status.

b. Genetic or biometric data.

c. Personal data of a known child.

d. Precise geolocation data.

(31) "Sexual assault" means any of the offenses defined in §§ 768–780 and § 787 of Title 11, or any equivalent provision in the laws of any other state, the United States, any territory, district, or subdivision of the United States, or any foreign jurisdiction.

(32) "Stalking" means the offense defined in § 1312 of Title 11, or any equivalent provision in the laws of any other state, the United States, any territory, district, or subdivision of the United States, or any foreign jurisdiction.

(33) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated Internet web sites or online applications to predict such consumer's preferences or interests. "Targeted advertising" does not include any of the following:

a. Advertisements based on activities within a controller's own Internet web sites or online applications.

b. Advertisements based on the context of a consumer's current search query, visit to an Internet web site, or online application.

c. Advertisements directed to a consumer in direct response to the consumer's request for information or feedback.

d. Processing personal data solely to measure or report advertising frequency, performance, or reach.

(34) "Third party" means, with respect to personal data controlled by a controller, any person other than the relevant consumer, the controller of such personal data, or a processor or an affiliate of the processor or the controller.

(35) "Trade secret" means as defined in § 2001(4) of Chapter 20 of this title.

(36) "Violent felony" means as defined in § 4201 of Title 11 and includes any equivalent provision in the laws of any other state, the United States, and territory, district, or subdivision of the United States, or any foreign jurisdiction.

§ 12D-103. Applicability of chapter.

(a) This chapter applies to persons that conduct business in the State or persons that produce products or services that are targeted to residents of the State and that during the preceding calendar year did any of the following:

(1) Controlled or processed the personal data of not less than 35,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction.

(2) Controlled or processed the personal data of not less than 10,000 consumers and derived more than 20 percent of their gross revenue from the sale of personal data.

(b) This chapter does not apply to any of the following entities:

(1) Any regulatory, administrative, advisory, executive, appointive, legislative, or judicial body of the State or a political subdivision of the State, including any board, bureau, commission, agency of the State or a political subdivision of the State, but excluding any institution of higher education.

(2) Any financial institution or affiliate of a financial institution, all as defined in 15 U.S.C. 6809, to the extent that the financial institution or affiliate is subject to Title V of the Gramm Leach Bliley Act (15 U.S.C. § 6801, et seq., as amended) and the rules and implementing regulations promulgated thereunder.

(3) Any nonprofit organization dedicated exclusively to preventing and addressing insurance crime.

(4) A national securities association registered pursuant to § 15A of the Securities Exchange Act of 1934 (15 U.S.C. § 78a, et seq., as amended) and the rules and implementing regulations promulgated thereunder, or a registered futures association so designated pursuant to § 17 of the Commodity Exchange Act (7 U.S.C. § 1, et seq., as amended) and the rules and implementing regulations promulgated thereunder.

(c) This chapter does not apply to the following information and data:

(1) Protected health information under HIPAA.

(2) Patient-identifying information for purposes of 42 U.S.C. § 290dd-2.

(3) Identifiable private information, as defined in 45 CFR § 46.102, to the extent that it is used for purposes of the federal policy for the protection of human subjects pursuant to 45 C.F.R. 46.

(4) Identifiable private information to the extent it is collected and used as part of human subjects research pursuant to the ICH E6 Good Clinical Practice Guideline issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use or the protection of human subjects under 21 CFR 50 and 56.

(5) Patient safety work product, as defined in 42 CFR 3.20, that is created and used for purposes of patient safety improvement pursuant to 42 C.F.R. 3, established pursuant to 42 U.S.C. §§ 299b–21 to 299b–26.

(6) Information to the extent it is used for public health, community health, or population health activities and purposes, as authorized by HIPAA, when provided by or to a Covered Entity or when provided by or to a Business Associate pursuant to a Business Associate Agreement with a Covered Entity.

(7) The collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, furnisher, or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the federal Fair Credit Reporting Act (15 U.S.C. § 1681, et seq., as amended).

(8) Personal data collected, processed, sold, or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721, et seq., as amended.

(9) Personal data regulated by the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, et seq., as amended.

(10) Personal data collected, processed, sold, or disclosed in compliance with the Farm Credit Act, 12 U.S.C. § 2001, et seq., as amended.

(11) Data processed or maintained in any of the following ways:

a. In the course of an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role.

b. As the emergency contact information of an individual, used for emergency contact purposes.

c. Necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under paragraph (11)a. of this subsection and used for the purposes of administering such benefits.

(12) Personal data collected, processed, sold, or disclosed in relation to price, route, or service, as such terms are used in the Airline Deregulation Act, 49 U.S.C. § 40101, et seq., as amended, by an air carrier subject to said act, to the extent any part of this chapter is preempted by the Airline Deregulation Act, 49 U.S.C. § 41713, as amended.

(13) Personal data of a victim of or witness to child abuse, domestic violence, human trafficking, sexual assault, violent felony, or stalking that is collected, processed, or maintained by a nonprofit organization that provides services to victims of or witnesses to child abuse, domestic violence, human trafficking, sexual assault, violent felony, or stalking.

(14) Data subject to Title V of the Gramm Leach Bliley Act (15 U.S.C. § 6801, et. seq., as amended) and the rules and implementing regulations promulgated thereunder.

(d) Controllers and processors that comply with the verifiable parental consent requirements of COPPA shall be deemed compliant with any obligation to obtain parental consent set forth in this chapter with respect to a consumer who is a child.

§ 12D-104. Consumer personal data rights.

(a) A consumer has the right to do all of the following:

(1) Confirm whether a controller is processing the consumer's personal data and access such personal data, unless such confirmation or access would require the controller to reveal a trade secret.

(2) Correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.

(3) Delete personal data provided by, or obtained about, the consumer.

(4) Obtain a copy of the consumer's personal data processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means, provided such controller shall not be required to reveal any trade secret.

(5) Obtain a list of the categories of third parties to which the controller has disclosed the consumer's personal data.

(6) Opt out of the processing of the personal data for purposes of any of the following:

a. Targeted advertising.

b. The sale of personal data, except as provided in subsection (b) of § 12D-106 of this chapter.

c. Profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

(b) A consumer may exercise rights under this section by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice. A consumer may designate an authorized agent in accordance with § 12D-105 of this chapter to exercise the rights of such consumer to opt out of the processing of such consumer's personal data for purposes of paragraph (a)(5) of this section on behalf of the consumer. In the case of processing personal data of a known child, the parent or legal guardian may exercise such consumer rights on the child's behalf. In the case of processing personal data concerning a consumer subject to a guardianship, conservatorship or other protective arrangement, the guardian or the conservator of the consumer may exercise such rights on the consumer's behalf.

(c) Except as otherwise provided in this chapter, a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to said sections as follows:

(1) A controller shall respond to the consumer without undue delay, but not later than 45 days after receipt of the request. The controller may extend the response period by 45 additional days when reasonably necessary, considering the complexity and number of the consumer's requests, provided the controller informs the consumer of any such extension within the initial 45-day response period and of the reason for the extension.

(2) If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than 45 days after receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision.

(3) Information provided in response to a consumer request shall be provided by a controller, free of charge, once per consumer during any 12-month period. If requests from a consumer are manifestly unfounded, excessive or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive or repetitive nature of the request.

(4) If a controller is unable to authenticate a request to exercise any of the rights afforded under paragraphs (1) through (5), inclusive, of subsection (a) of this section using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action pursuant to this section and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise such right or rights until such consumer provides additional information reasonably necessary to authenticate such consumer and such consumer's request to exercise such right or rights. A controller shall not be required to authenticate an opt-out request, but a controller may deny an opt-out request if the controller has a good faith, reasonable, and documented belief that such request is fraudulent. If a controller denies an opt-out request because the controller believes such request is fraudulent, the controller shall send a notice to the person who made such request disclosing that such controller believes such request is fraudulent, why such controller believes such request is fraudulent, and that such controller shall not comply with such request.

(5) A controller that has obtained personal data about a consumer from a source other than the consumer shall be deemed in compliance with a consumer's request to delete such data pursuant to paragraph (3) of subsection (a) of this section if the controller retains a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the controller's records and does not use such retained data for any other purpose.

(d) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Not later than 60 days after receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Department of Justice to submit a complaint.

§ 12D-105. Designation of agent to exercise rights of consumer, including through universal opt-out mechanisms.

(a) A consumer may designate an authorized agent to act on the consumer's behalf to opt out of the processing of such consumer's personal data for one or more of the purposes specified in paragraph (a)(5) of § 12D-104 of this chapter. The consumer may designate such authorized agent by way of, among other things, a platform, technology, or mechanism, including an Internet link or a browser setting, browser extension, or global device setting, indicating such consumer's intent to opt out of such processing. For the purposes of such designation, the platform, technology, or mechanism may function as the agent for purposes of conveying the consumer's decision to opt-out.

(b) A controller shall comply with an opt-out request received from an authorized agent if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on such consumer's behalf. The Department of Justice may publish or reference on its website a list of agents who presumptively shall have such authority unless the controller has established a reasonable basis to conclude that the agent lacks such authority.

§ 12D-106. Duties of controllers.

(a) A controller shall do all of the following:

(1) Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer.

(2) Except as otherwise permitted by this chapter, not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.

(3) Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue.

(4) Not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without first obtaining consent from the child's parent or lawful guardian and otherwise complying with § 1204C of Chapter 12C of this title.

(5) Not process personal data in violation of the laws of this State and federal laws that prohibit unlawful discrimination.

(6) Provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, upon revocation of such consent, cease to process the data as soon as practicable, but not later than 15 days after the receipt of such request.

(7) Not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data without the consumer's consent, under circumstances where a controller has actual knowledge or willfully disregards that the consumer is at least thirteen years of age but younger than 18 years of age.

(8) Not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer.

(b) Nothing in subsection (a) of this section shall be construed to require a controller to provide a product or service that requires the personal data of a consumer which the controller does not collect or maintain, or prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

(c) A controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes all of the following:

(1) The categories of personal data processed by the controller.

(2) The purpose for processing personal data.

(3) How consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request.

(4) The categories of personal data that the controller shares with third parties, if any.

(5) The categories of third parties with which the controller shares personal data, if any.

(6) An active electronic mail address or other online mechanism that the consumer may use to contact the controller.

(d) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing.

(e)(1) A controller shall establish, and shall describe in the privacy notice required by subsection (c) of this section, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights pursuant to this chapter. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests, and the ability of the controller to verify the identity of the consumer making the request. A controller shall not require a consumer to create a new account in order to exercise consumer rights, but may require a consumer or the consumer's authorized agent to use an existing account. Any such means shall include all of the following:

a.1. Providing a clear and conspicuous link on the controller's Internet web site to an Internet web page that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising or the sale of the consumer's personal data.

2. Not later than [one year following the effective date of this Act], allowing a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data, through an opt-out preference signal sent, with such consumer's consent, by a platform, technology, or mechanism to the controller indicating such consumer's intent to opt out of any such processing or sale. Such platform, technology, or mechanism shall do all of the following:

A. Not unfairly disadvantage another controller.

B. Not make use of a default setting, but, rather, require the consumer to make an affirmative, freely given, and unambiguous choice to opt out of any processing of such consumer's personal data pursuant to this chapter.

C. Be consumer-friendly and easy to use by the average consumer.

D. Be as consistent as possible with any other similar platform, technology, or mechanism required by any federal or state law or regulation.

E. Enable the controller to reasonably determine whether the consumer is a resident of the State and whether the consumer has made a legitimate request to opt out of any sale of such consumer's personal data or targeted advertising.

b. If a consumer's decision to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data, through an opt-out preference signal sent in accordance with the provisions of paragraph (1)a. of this subsection conflicts with the consumer's existing controller-specific privacy setting or voluntary participation in a controller's bona fide loyalty, rewards, premium features, discounts or club card program, the controller shall comply with such consumer's opt-out preference signal but may notify such consumer of such conflict and provide to such consumer the choice to confirm such controller-specific privacy setting or participation in such program.

(2) If a controller responds to consumer opt-out requests received pursuant to paragraph (1)a. of this subsection by informing the consumer of a charge for the use of any product or service, the controller shall present the terms of any financial incentive offered pursuant to paragraph (1)b. of this subsection for the retention, use, sale, or sharing of the consumer's personal data.

§ 12D-107. Duties of processors.

(a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under this chapter. Such assistance must include all of the following:

(1) Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests.

(2) Taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security, as defined in § 12B-101(1) of Chapter 12B of this title, of the system of the processor, in order to meet the controller's obligations.

(3) Providing necessary information to enable the controller to conduct and document data protection assessments.

(b) A contract between a controller and a processor must govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract must be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties. The contract must also require that the processor to do all of the following:

(1) Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data.

(2) At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law.

(3) Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this chapter.

(4) After providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

(5) Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this chapter, using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request.

(c) Nothing in this section may be construed to relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of such controller's or processor's role in the processing relationship, as described in this chapter.

(d) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A person who is not limited in such person's processing of personal data pursuant to a controller's instructions, or who fails to adhere to such instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to such processing and may be subject to an enforcement action under this chapter.

§ 12D-108. Data protection assessments.

(a) A controller that controls or processes the data of not less than 100,000 consumers, excluding data controlled or processed solely for the purpose of completing a payment transaction, shall conduct and document, on a regular basis, a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer. For the purposes of this section, processing that presents a heightened risk of harm to a consumer includes any of the following:

(1) The processing of personal data for the purposes of targeted advertising.

(2) The sale of personal data.

(3) The processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of any of the following:

a. Unfair or deceptive treatment of, or unlawful disparate impact on, consumers.

b. Financial, physical, or reputational injury to consumers.

c. A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person.

d. Other substantial injury to consumers.

(4) The processing of sensitive data.

(b) Data protection assessments conducted pursuant to subsection (a) of this section shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The controller shall factor into any such data protection assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

(c) The Attorney General may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in this chapter. Data protection assessments must be treated as confidential and are not public records within the meaning of § 10002(o) of Chapter 100 of Title 29. Notwithstanding the foregoing, a controller's data

protection assessment may be used in an action to enforce this chapter. To the extent any information contained in a data protection assessment disclosed to the Attorney General includes and conspicuously identifies information subject to attorney-client privilege or work product protection, such disclosure by itself does not constitute a waiver of such privilege or protection.

(d) A single data protection assessment may address a comparable set of processing operations that include similar activities.

(e) If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment shall be deemed to satisfy the requirements established in this section if such data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.

(f) Data protection assessment requirements shall apply to processing activities created or generated on or after [six months following the effective date of this chapter] and are not retroactive.

§ 12D-109. De-identified data.

(a) Nothing in this chapter shall be construed to require a controller or processor to re-identify de-identified data or pseudonymous data, or to maintain data in identifiable form, or collect, obtain, retain, or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data.

(b) Nothing in this chapter shall be construed to require a controller or processor to comply with an authenticated consumer rights request if all of the following apply:

(1) The controller is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data.

(2) The controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer.

(3) The controller does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.

(c) The rights afforded under paragraphs (1) to (4), inclusive, of subsection (a) of § 12D-104 of this chapter do not apply to pseudonymous data in cases where the controller is able to demonstrate that any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.

(d) A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments. The determination of the reasonableness of such oversight and the appropriateness of contractual enforcement must take into account whether the disclosed data includes data that would be sensitive data if it were re-identified.

§ 12D-110. Exclusions.

(a) Nothing in this chapter shall be construed to restrict a controller's or processor's ability to do any of the following:

(1) Comply with federal, state, or local laws, rules, or regulations.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities.

(3) Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations.

(4) Investigate, establish, exercise, prepare for, or defend legal claims.

(5) Provide a product or service specifically requested by a consumer.

(6) Perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty.

(7) Take steps at the request of a consumer prior to entering into a contract.

(8) Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual, and where the processing cannot be manifestly based on another legal basis.

(9) Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity, preserve the integrity or security of systems, or investigate, report or prosecute those responsible for any such activity.

(10) Engage in public or peer-reviewed scientific research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board that determines whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller, the expected benefits of the research outweigh the privacy risks, and whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification.

(11) Assist another controller, processor, or third party with any of the activities under this subsection.

(b) The obligations imposed on controllers or processors under this chapter, other than those imposed by § 12D-109 of this chapter, do not restrict a controller's or processor's ability to collect consumer data, or use or retain such data, for internal use only, to do any of the following:

(1) Conduct internal research to develop, improve or repair products, services or technology.

(2) Effectuate a product recall.

(3) Identify and repair technical errors that impair existing or intended functionality.

(4) Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller, or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

(c) The obligations imposed on controllers or processors under this chapter shall not apply where compliance by the controller or processor with said sections would violate an evidentiary privilege under the laws of this State. Nothing in this chapter shall be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of this State as part of a privileged communication.

(d) A controller or processor that discloses personal data to a processor or third-party controller in compliance with this chapter shall not be deemed to have violated said sections if the processor or third-party controller that receives and processes such personal data violates said sections, provided that (i) at the time the disclosing controller or processor disclosed such personal data, the disclosing controller or processor did not have actual knowledge that the receiving processor or third-party controller had violated or would violate said sections and (ii) the disclosing controller or processor

was, and remained, in compliance with its obligations as the discloser of such data hereunder. A third-party controller or processor receiving personal data from a controller or processor in compliance with this chapter is likewise not in violation of said sections for the independent misconduct of the controller or processor from which such third-party controller or processor receives such personal data.

(e) Nothing in this chapter may be construed to do any of the following:

(1) Impose any obligation on a controller or processor that adversely affects the rights of any person to freedom of speech or freedom of the press guaranteed in the First Amendment to the United States Constitution or § 5 of Article I of the Delaware Constitution of 1897.

(2) Apply to any person's processing of personal data in the course of such person's purely personal or household activities.

(f) Personal data processed pursuant to this section may be processed to the extent that such processing is reasonably necessary and proportionate to the purposes listed in this section, and is adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section. Personal data collected, used, or retained pursuant to subsection (b) of this section shall, where applicable, take into account the nature and purpose or purposes of such collection, use, or retention. Such data shall be subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to such collection, use, or retention of personal data.

(g) If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in subsection (f) of this section.

(h) Processing personal data for the purposes expressly identified in this section shall not solely make a legal entity a controller with respect to such processing.

§ 12D-111. Enforcement.

(a) The Department of Justice has enforcement authority over this chapter and may investigate and prosecute violations of this chapter in accordance with the provisions of Subchapter II of Chapter 25 of Title 29.

(b) During the period beginning on [the effective date of this act], and ending on December 31, 2025, the Department of Justice shall, prior to initiating any action for a violation of any provision of this chapter, issue a notice of violation to the controller if the Department of Justice determines that a cure is possible. If the controller fails to cure such violation within 60 days of receipt of the notice of violation, the Department of Justice may bring an enforcement proceeding pursuant to subsection (a) of this section.

(c) Beginning on January 1, 2026, the Department of Justice may, in determining whether to grant a controller or processor the opportunity to cure an alleged violation of any provision of this chapter, the Department of Justice may consider all of the following:

(1) The number of violations.

(2) The size and complexity of the controller or processor.

(3) The nature and extent of the controller's or processor's processing activities.

(4) The substantial likelihood of injury to the public.

(5) The safety of persons or property.

(6) Whether such alleged violation was likely caused by human or technical error.

(7) The extent to which the controller or processor has violated this or similar laws in the past.

(d) Nothing in this chapter shall be construed as providing the basis for, or be subject to, a private right of action for violations of said sections or any other law.

(e) A violation of this chapter shall be deemed an unlawful practice under § 2513 of Chapter 25 of this title and a violation of Subchapter II of Chapter 25 of this title, and shall be enforced solely by the Department of Justice.

Section 2. Beginning at least 6 months prior to the effective date of this Act, the Department of Justice shall engage in public outreach to educate consumers and the business community about the Act.

Section 3. If this Act is enacted before or on January 1, 2024, this Act takes effect on January 1, 2025. If this Act is enacted after January 1, 2024, this Act takes effect on January 1, 2026.

Section 4. If any provision of this Act or the application thereof to any person or circumstances is held invalid, the invalidity does not affect any other provision or application of the Act which can be given effect without the invalid provision or application; and, to that end, the provisions of this Act are declared to be severable.

Indiana Code Concerning Trade Regulation

SECTION 1. IC 24-15 IS ADDED TO THE INDIANA CODE AS A NEW ARTICLE TO READ AS FOLLOWS [EFFECTIVE JANUARY 1, 2026]:

ARTICLE 15. CONSUMER DATA PROTECTION

Chapter 1. Applicability

Sec. 1. (a) This article applies to a person that conducts business in Indiana or produces products or services that are targeted to residents of Indiana and that during a calendar year:

(1) controls or processes personal data of at least one hundred thousand (100,000) consumers who are Indiana residents; or

(2) controls or processes personal data of at least twenty-five thousand (25,000) consumers who are Indiana residents and derives more than fifty percent (50%) of gross revenue from the sale of personal data.

(b) This article does not apply to any of the following:

(1) Either of the following:

(A) The state, a state agency, or a body, authority, board, bureau, commission, district, or agency of any political subdivision of the state.

(B) A third party under contract with an entity described in clause (A), when acting on behalf of the entity. This clause does not exempt data held or created by third parties outside of the scope of the contract with the entity.

(2) Any financial institutions and affiliates, or data subject to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.).

(3) Any covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services (45 CFR Parts 160 and 164) pursuant to HIPAA.

(4) Any nonprofit organization.

(5) Any institution of higher education.

(6) Any public utility (as defined in IC 8-1-2-1(a)) or service company affiliated with a public utility (as defined in IC 8-1-2-1(a)). For purposes of this subdivision, "service company" means an associate company within a holding company system organized specifically for the purpose of providing goods or services to a public utility (as defined in IC 8-1-2-1(a)) in the same holding company system.

Sec. 2. The following information and data are exempt from this article:

(1) Protected health information under HIPAA and related regulations under 45 CFR Part 160, 45 CFR Part 162, and 45 CFR Part 164.

(2) Patient identifying information for purposes of 42 U.S.C. 290dd-2.

(3) Any of the following:

(A) Identifiable private information for purposes of the federal policy for the protection of human subjects under 45 CFR Part 46.

(B) Identifiable private information that is otherwise information collected as part of human subjects research under the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use.

(C) The protection of human subjects under 21 CFR Parts 50 and 56.

(D) Personal data used or shared in research conducted in accordance with the requirements set forth in this article.

(E) Other research conducted in accordance with applicable law.

(4) Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986 (42 U.S.C. 11101 et seq.).

(5) Patient safety work product for purposes of the federal Patient Safety and Quality Improvement Act (42 U.S.C. 299b-21 et seq.).

(6) Information derived from any of the health care related information set forth in this section that is de-identified in accordance with the requirements for de-identification under HIPAA.

(7) Information:

(A) originating from;

(B) intermingled with so as to be indistinguishable from; or

(C) treated in the same manner as; information that is exempt under this section and that is maintained by a covered entity or business associate, as defined in HIPAA, or a program or qualified service organization under 42 U.S.C. 290dd-2.

(8) Information used only for public health activities and purposes, as authorized by HIPAA.

(9) The collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by:

(A) a consumer reporting agency, furnisher, or user that provides information for use in a consumer report; or

(B) a user of a consumer report; but only to the extent that such activity is regulated by and authorized under the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

(10) Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. 2721 et seq.).

(11) Personal data regulated by the federal Family Educational Rights and Privacy Act (20 U.S.C. 1232g et seq.).

(12) Personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act (12 U.S.C. 2001 et seq.).

(13) Data processed or maintained:

(A) in the course of an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role;

(B) as emergency contact information for an individual under this article and used for emergency contact purposes; or

(C) that is necessary to retain to administer benefits for another individual relating to the individual under clause (A) and used for the purposes of administering those benefits.

Sec. 3. A:

(1) controller; or

(2) processor; that complies with the Children's Online Privacy Protection Act (15 U.S.C. 6501 et seq.), and with any rules or regulations under that act, satisfies any obligation to obtain parental consent under this article.

Chapter 2. Definitions

Sec. 0.5. The definitions in this chapter apply throughout this article.

Sec. 1. (a) "Affiliate" means a legal entity that:

(1) controls, is controlled by, or is under common control with another legal entity; or

(2) shares common branding with another legal entity.

(b) For purposes of this section, "control", with respect to a company, means:

(1) ownership of, or the power to vote, more than fifty percent (50%) of the outstanding shares of any class of voting security of the company;

(2) control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or

(3) the power to exercise controlling influence over the management of the company.

Sec. 2. "Aggregate data" means information:

(1) that relates to a group or category of consumers;

(2) from which individual consumer identities have been removed; and

(3) that is not linked or reasonably linkable to any consumer.

Sec. 3. "Authenticate" means to verify through reasonable means that a consumer who is entitled to exercise the personal data rights provided by IC 24-15-3 is the same consumer exercising such rights with respect to particular personal data.

Sec. 4. (a) "Biometric data" means data that:

(1) is generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, images of the retina or iris, or other unique biological patterns or characteristics; and

(2) is used to identify a specific individual.

(b) The term does not include:

(1) a physical or digital photograph, or data generated from a physical or digital photograph;

(2) a video or audio recording, or data generated from a video or audio recording; or

(3) information collected, used, or stored for health care treatment, payment, or operations under HIPAA.

Sec. 5. "Business associate" has the meaning set forth in 45 CFR 160.103.

Sec. 6. “Child” means any individual who is less than thirteen (13) years of age.

Sec. 7. (a) “Consent” means a clear affirmative act that signifies a consumer’s freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer.

(b) For purposes of this section, a “clear affirmative act” includes a written statement, including a statement written by electronic means, or any other unambiguous affirmative action.

Sec. 8. (a) “Consumer” means an individual who:

(1) is a resident of Indiana; and

(2) is acting only for a personal, family, or household purpose.

(b) The term does not include an individual acting in a commercial or employment context.

Sec. 9. “Controller” means a person that, alone or jointly with others, determines the purpose and means of processing personal data.

Sec. 10. “Covered entity” has the meaning set forth in 45 CFR 160.103.

Sec. 11. “Decision that produces legal or similarly significant effects concerning a consumer” means a decision made by a controller that results in the provision or denial by the controller of:

(1) financial and lending services;

(2) housing;

(3) insurance;

(4) education enrollment;

(5) criminal justice;

(6) employment opportunities;

(7) health care services; or

(8) access to basic necessities, such as food and water.

Sec. 12. “De-identified data” means data that cannot reasonably be linked to an identified or identifiable individual because a controller that possesses the data:

(1) takes reasonable measures to ensure that the data cannot be associated with an individual;

(2) publicly commits to maintaining and using the data without attempting to re-identify the data; and

(3) obligates any recipients of the data through contractual requirements to comply with all applicable provisions of this article.

Sec. 13. “Health care provider” has the meaning set forth in IC 4-6-14-2.

Sec. 14. “Health record” has the meaning set forth in IC 1-1-4-5(a)(6).

Sec. 15. “HIPAA” refers to the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d et seq.).

Sec. 16. “Identified or identifiable individual” means an individual who can be readily identified, directly or indirectly.

Sec. 17. “Institution of higher education” means a public or private college or university.

Sec. 18. “Nonprofit organization” means any organization exempt from taxation under Section 501(c)(3), 501(c)(6), or 501(c)(12) of the Internal Revenue Code.

Sec. 19. (a) “Personal data” means information that is linked or reasonably linkable to an identified or identifiable individual.

(b) The term does not include:

(1) de-identified data;

(2) aggregate data; or

(3) publicly available information.

Sec. 20. (a) “Precise geolocation data” means information derived from technology, including global positioning system level latitude and longitude coordinates, that directly identifies the specific location of a natural person with precision and accuracy within a radius of one thousand seven hundred fifty (1,750) feet.

(b) The term does not include:

(1) the content of communications; or

(2) any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

Sec. 21. “Processing”, with respect to personal data, means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

Sec. 22. “Processor” means a person that processes personal data on behalf of a controller.

Sec. 23. “Profiling” means any form of solely automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual’s economic situation, health or health records, personal preferences, interests, reliability, behavior, location, or movements.

Sec. 24. “Protected health information” has the meaning set forth in 45 CFR 160.103.

Sec. 25. “Pseudonymous data” means personal data that cannot be attributed to a specific individual because additional information that would allow the data to be attributed to a specific individual is:

(1) kept separately; and

(2) subject to appropriate technical and organizational measures; to ensure that the personal data is not attributed to an identified or identifiable individual.

Sec. 26. “Publicly available information” means information:

(1) that is lawfully made available through federal, state, or local government records; or

(2) that a business has a reasonable basis to believe is lawfully made available:

(A) to the general public through widely distributed media;

(B) by the consumer to whom the information pertains; or

(C) by a person to whom the consumer has disclosed the information; unless the consumer has restricted the information to a specific audience.

Sec. 27. (a) "Sale of personal data" means the exchange of personal data for monetary consideration by a controller to a third party.

(b) The term does not include:

(1) the disclosure of personal data to a processor that processes the personal data on behalf of the controller;

(2) the disclosure of personal data to a third party for purposes of providing a product or service requested by:

(A) the consumer; or

(B) the parent of a child; to whom the personal data pertains;

(3) the disclosure or transfer of personal data to an affiliate of the controller;

(4) the disclosure of information that the consumer:

(A) intentionally made available to the general public via a channel of mass media; and

(B) did not restrict to a specific audience; or

(5) the disclosure or transfer of personal data to a third party as an asset that is part of a proposed or actual merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

Sec. 28. "Sensitive data" means a category of personal data that includes any of the following:

(1) Personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health diagnosis made by a health care provider, sexual orientation, or citizenship or immigration status.

(2) Genetic or biometric data that is processed for the purpose of uniquely identifying a specific individual.

(3) Personal data collected from a known child.

(4) Precise geolocation data.

Sec. 29. "State agency" has the meaning set forth in IC 1-1-15-3.

Sec. 30. (a) "Targeted advertising" means the displaying of an advertisement to a consumer in which the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests.

(b) The term does not include:

(1) advertisements based on activities within a controller's own or affiliated websites or online applications;

(2) advertisements based on the context of a consumer's current search query, visit to a website, or online application;

(3) advertisements directed to a consumer in response to the consumer's request for information or feedback; or

(4) the processing of personal data solely for measuring or reporting advertising performance, reach, or frequency.

Sec. 31. "Third party", with respect to a context to which this article applies, means a natural or legal person, public authority, agency, or body other than:

(1) the consumer;

(2) the controller;

(3) the processor; or

(4) an affiliate of the processor or the controller.

Sec. 32. "Trade secret" has the meaning set forth in IC 24-2-3-2.

Chapter 3. Personal Data; Consumer Rights

Sec. 1. (a) A consumer may invoke one (1) or more rights set forth in subsection (b) by submitting to a controller a request specifying the rights the consumer wishes to invoke. A known child's parent or legal guardian may invoke on behalf of the child one (1) or more rights set forth in subsection (b) with respect to the processing of personal data belonging to the known child by submitting to a controller a request specifying the rights the consumer wishes to invoke on behalf of the child. Except as provided in IC 24-15-7-1(c) and IC 24-15-7-2, and subject to any limitations or conditions set forth in subsections (b) and (c), a controller shall comply with an authenticated consumer request to exercise a right set forth in subsection (b).

(b) A consumer has the following rights:

(1) To confirm whether or not a controller is processing the consumer's personal data and, subject to the limitations set forth in subdivision (4), to access such personal data.

(2) To correct inaccuracies in the consumer's personal data that the consumer previously provided to a controller, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data. Upon receiving a request from a consumer under this subdivision, a controller shall correct inaccurate information as requested by the consumer, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.

(3) To delete personal data provided by or obtained about the consumer.

(4) To obtain either:

(A) a copy of; or

(B) a representative summary of; the consumer's personal data that the consumer previously provided to the controller. Information provided to a consumer under this subdivision must be in a portable and, to the extent technically practicable, readily usable format that allows the consumer to transmit the data or summary to another controller without hindrance, in any case in which the processing is carried out by automated means. The controller has the discretion to send either a copy or a representative summary of the consumer's personal data under this subdivision, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data. A controller is not required to provide a copy or a representative summary of a consumer's personal data to the same consumer under this subdivision more than one (1) time in a twelve (12) month period.

(5) To opt out of the processing of the consumer's personal data for purposes of:

(A) targeted advertising;

(B) the sale of personal data; or

(C) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

(c) Except as otherwise provided in this article, a controller shall comply with a request by a consumer to exercise a consumer right set forth in subsection (b) as follows:

(1) A controller shall respond to the consumer without undue delay, but in any case not later than forty-five (45) days after receipt of the consumer's request under this section. The response period prescribed by this subdivision may be extended once by an additional forty-five (45) days when reasonably necessary, taking into account the complexity and number of the consumer's requests, as long as the controller informs the consumer of any such extension within the initial forty-five (45) day response period, along with the reason for the extension.

(2) If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but in any case not later than forty-five (45) days after receipt of the consumer's request under this section, of the justification for declining to take action, and shall provide instructions for how to appeal the decision under subsection (d).

(3) Information provided in response to a consumer request shall be provided by a controller free of charge, up to one (1) time annually per consumer. If requests from a consumer are manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of the request.

(4) If a controller is unable to authenticate the request using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action under this section and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.

(5) A controller that has obtained personal data about a consumer from a source other than the consumer is considered to comply with a request by the consumer under subsection (b)(3) to delete the consumer's personal data if the controller:

(A) retains:

(i) a record of the consumer's request for deletion; and

(ii) the minimum data necessary to ensure that the consumer's personal data remains deleted from the controller's records; and

(B) does not use the data retained under clause (A)(ii) for any other purpose.

(d) A controller shall establish a process for a consumer to appeal, within a reasonable period of time after the consumer's receipt of a decision by the controller under subsection (c)(2), the controller's refusal to take action on a request by the consumer under this section. The appeal process shall be conspicuously available and similar to the process for submitting requests to invoke a right under this section. Not later than sixty (60) days after receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general to submit a complaint.

Chapter 4. Data Controller Responsibilities; Transparency

Sec. 1. Except as provided in IC 24-15-7-2, a controller has the following responsibilities:

(1) A controller shall limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer.

(2) Except as otherwise provided in this article, a controller shall not process personal data for purposes that are neither reasonably necessary for nor compatible with the disclosed purposes for which the personal data is processed, unless the controller obtains the consumer's consent.

(3) A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. The data security practices required under this subdivision must be appropriate to the volume and nature of the personal data at issue.

(4) A controller shall not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising any of the consumer rights set forth in this article, including by denying goods or services to the consumer, charging different prices or rates for goods and services, or providing a different level or quality of goods or services to the consumer. However, nothing in this subdivision shall be construed to:

(A) require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain; or

(B) prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised the consumer's right to opt out under IC 24-15-3-1(b)(5) or if the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discount, or club card program.

(5) A controller shall not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with the federal Children's Online Privacy Protection Act (15 U.S.C. 6501 et seq.).

Sec. 2. Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under IC 24-15-3 is contrary to public policy and is void and unenforceable.

Sec. 3. A controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

(1) the categories of personal data processed by the controller;

(2) the purpose for processing personal data;

(3) how consumers may exercise their consumer rights under IC 24-15-3, including how a consumer may appeal a controller's decision with regard to the consumer's request;

(4) the categories of personal data that the controller shares with third parties, if any; and

(5) the categories of third parties, if any, with whom the controller shares personal data.

Sec. 4. If a controller sells a consumer's personal data to third parties or uses a consumer's personal data for targeted advertising, the controller shall clearly and conspicuously disclose such activity, as well as the manner in which a consumer may exercise the right to opt out of such sales or use.

Sec. 5. A controller shall establish, and shall describe in a privacy notice provided under section 3 of this chapter, one (1) or more secure and reliable means for consumers to submit a request to exercise their rights under IC 24-15-3. Such means must take into account:

(1) the ways in which consumers normally interact with the controller;

(2) the need for the secure and reliable communication of such requests; and

(3) the ability of the controller to authenticate the identity of the consumer making the request. A controller may not require a consumer to create a new account in order to exercise the consumer's rights under IC 24-15-3 but may require a consumer to use an existing account.

Sec. 6. The attorney general may maintain on the attorney general's website a list of resources for controllers, including sample privacy notices and disclosures, to assist controllers in complying with this chapter.

Chapter 5. Responsibility According to Role; Controllers and Processors

Sec. 1. A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under this chapter. Such assistance shall include the following:

(1) Assisting the controller in meeting the controller's obligation to respond to consumer requests under IC 24-15-3 by appropriate technical and organizational measures, insofar as this is reasonably practicable, and taking into account the nature of processing and the information available to the processor.

(2) Taking into account the nature of processing and the information available to the processor, assisting the controller in meeting the controller's obligations in relation to:

(A) the security of processing the personal data; and

(B) the notification of a breach of security of the system of the processor under IC 24-4.9; in order to meet the controller's obligations.

(3) Providing necessary information to enable the controller to conduct and document data protection impact assessments under IC 24-15-6.

Sec. 2. (a) A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract must be binding and clearly set forth instructions for processing personal data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract must also include requirements that the processor do the following:

(1) Ensure that each individual processing personal data is subject to a duty of confidentiality with respect to the data.

(2) At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law.

(3) Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this chapter.

(4) Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor. Alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the processor's obligations under this chapter using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of any such assessment to the controller upon request.

(5) Subject to subsection (b), engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

(b) Nothing in this section shall be construed to relieve a controller or a processor from the liabilities imposed on the controller or processor by virtue of its role in the processing relationship.

Sec. 3. Determining whether a person is acting as a controller or a processor with respect to a specific processing of data is a fact based determination that depends upon the context in which personal data is processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor.

Chapter 6. Data Protection Impact Assessments

Sec. 1. (a) The data protection impact assessment requirements set forth in this chapter apply to processing activities created or generated after December 31, 2025, and are not retroactive to any processing activities created or generated before January 1, 2026.

(b) A controller shall conduct and document a data protection impact assessment of each of the following processing activities involving personal data:

(1) The processing of personal data for purposes of targeted advertising.

(2) The sale of personal data.

(3) The processing of personal data for purposes of profiling, if such profiling presents a reasonably foreseeable risk of:

(A) unfair or deceptive treatment of, or unlawful disparate impact on, consumers;

(B) financial, physical, or reputational injury to consumers;

(C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, if such intrusion would be offensive to a reasonable person; or

(D) other substantial injury to consumers.

(4) The processing of sensitive data.

(5) Any processing activities involving personal data that present a heightened risk of harm to consumers.

(c) Data protection impact assessments conducted under this chapter shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, shall be factored into this assessment by the controller.

(d) A single data protection impact assessment may address a comparable set of processing operations that include similar activities.

(e) A data protection impact assessment conducted by a controller for the purpose of compliance with other laws or regulations may be used to comply with this section if the assessment has a reasonably comparable scope and effect to an assessment conducted under this section.

Sec. 2. (a) The attorney general may request, pursuant to a civil investigative demand, that a controller disclose any data protection impact assessment that is relevant to an investigation conducted by the attorney general. Upon receipt of such a request, the controller shall make the data protection impact assessment available to the attorney general. Subject to subsection (b), the attorney general may evaluate the data protection impact assessment for a controller's compliance with the responsibilities set forth in IC 24-15-4.

(b) Data protection impact assessments are confidential and exempt from public inspection and copying under IC 5-14-3-4. The disclosure of a data protection impact assessment pursuant to a request from the attorney general does not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

Chapter 7. Processing De-identified Data or Pseudonymous Data; Exemptions

Sec. 1. (a) A controller in possession of de-identified data shall:

(1) take reasonable measures to ensure that the data cannot be associated with an individual;

(2) publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and

(3) contractually obligate any recipients of the de-identified data to comply with all provisions of this chapter.

(b) This chapter shall not be construed to require a controller or processor to:

(1) re-identify de-identified data or pseudonymous data;

(2) maintain data in identifiable form; or

(3) collect, obtain, retain, or access any data or technology; in order to be capable of associating an authenticated consumer request with personal data.

(c) This chapter shall not be construed to require a controller or processor to comply with a request of a consumer under IC 24-15-3 if all of the following conditions are met:

(1) The controller is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data.

(2) The controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer.

(3) The controller does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor.

Sec. 2. The:

(1) rights of a consumer set forth in IC 24-15-3-1(b)(1) through IC 24-15-3-1(b)(4); and

(2) responsibilities of a controller under IC 24-15-4-1(1) through IC 24-15-4-1(5); do not apply to pseudonymous data in any case in which the controller is able to demonstrate that any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.

Sec. 3. A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

Chapter 8. Limitations

Sec. 1. (a) This article shall not be construed to restrict a controller's or processor's ability to do any of the following:

(1) Comply with federal, state, or local laws, rules, or regulations or, in the case of an owner of a riverboat licensed under IC 4-33-6, implement and operate a facial recognition program approved by the Indiana gaming commission.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, state, local, or other governmental authority.

(3) Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations.

(4) Investigate, establish, exercise, prepare for, or defend legal claims.

(5) Provide a product or service specifically requested by a consumer, perform a contract to which the consumer, or a parent of a child, is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer or parent before entering into a contract.

(6) Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another individual, if the processing cannot be manifestly based on another legal basis.

(7) Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity, investigate, report, or prosecute those responsible for any such action, and preserve the integrity or security of systems.

(8) Engage in public or peer reviewed scientific or statistical research that is in the public interest and that adheres to all applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, or a similar independent oversight entity, that determines if:

(A) the information is likely to provide substantial benefits that do not exclusively accrue to the controller;

(B) the expected benefits of the research outweigh the privacy risks; and

(C) the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification.

(9) Assist another controller, processor, or third party with any obligation described in this section.

(b) Processing personal data for a purpose expressly identified in subsection (a)(1) through (a)(9) does not by itself make a person a controller with respect to such processing.

Sec. 2. The obligations imposed on a controller or a processor under this article do not prohibit or restrict a controller or processor from collecting, using, or retaining data to do the following:

(1) Conduct internal research to develop, improve, or repair products, services, or technology.

(2) Effectuate a product recall.

(3) Identify and repair technical errors that impair existing or intended functionality.

(4) Perform internal operations that are:

(A) reasonably compatible with the expectations of the consumer;

(B) reasonably anticipated based on the consumer's existing relationship with the controller; or

(C) otherwise compatible with:

(i) processing data in furtherance of the provision of a product or service specifically requested by a consumer, or the parent of a child; or

(ii) the performance of a contract to which the consumer is a party.

Sec. 3. The obligations imposed on a controller or a processor under this article do not apply if compliance by the controller or processor with this article would violate an evidentiary privilege under Indiana law. This article shall not be construed to prohibit a controller or processor from providing, as part of a privileged communication, personal data concerning a consumer to a person covered by an evidentiary privilege under Indiana law.

Sec. 4. A controller or processor that discloses personal data to a third party controller or processor in compliance with this article is not in violation of this article if the third party controller or processor that receives and processes the personal data violates this article, as long as, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation. A third party controller or processor receiving personal data from a controller or processor is likewise not in violation of this article solely because of the transgressions of the controller or processor from which it receives such personal data.

Sec. 5. This article:

(1) shall not be construed as an obligation imposed on controllers and processors that adversely affects the rights or freedoms of any persons, such as exercising the right of free speech under the First Amendment to the Constitution of the United States; and

(2) does not apply to personal data in the context of a purely personal or household activity.

Sec. 6. Nothing in this article shall be construed as requiring a controller to disclose trade secrets.

Sec. 7. (a) Personal data processed by a controller for a purpose authorized under this chapter may not be processed for any other purpose unless otherwise allowed under this article. Personal data processed by a controller under this chapter may be processed to the extent that such processing is:

(1) reasonably necessary and proportionate to a purpose authorized under this chapter; and

(2) adequate, relevant, and limited to what is necessary in relation to the specific purpose.

(b) Personal data collected, used, or retained under section 2 of this chapter:

(1) shall, as applicable, take into account the nature and purpose of the collection, use, or retention; and

(2) must be subject to reasonable administrative, technical, and physical measures to:

(A) protect the confidentiality, integrity, and accessibility of the personal data; and

(B) reduce reasonably foreseeable risks of harm to consumers relating to such collection, use, or retention of the personal data.

(c) If a controller processes personal data pursuant to an exemption under this chapter, the controller bears the burden of demonstrating that such processing:

(1) qualifies for the exemption; and

(2) complies with the requirements set forth in this section.

Chapter 9. Investigative Authority

Sec. 1. Whenever the attorney general has reasonable cause to believe that any person has engaged in, is engaging in, or is about to engage in any violation of this article, the attorney general is empowered to issue a civil investigative demand to investigate the suspected violation.

Chapter 10. Enforcement

Sec. 1. The attorney general has exclusive authority to enforce the provisions of this article.

Sec. 2. (a) The attorney general may initiate an action in the name of the state and may seek an injunction to restrain any violations of this article and a civil penalty not to exceed seven thousand five hundred dollars ($7,500) for each violation under this article.

(b) The attorney general may recover reasonable expenses incurred in investigating and preparing the case, including attorney's fees, in any action initiated under this chapter.

Sec. 3. (a) Before initiating an action under section 2 of this chapter, the attorney general shall provide a controller or processor thirty (30) days written notice identifying the specific provisions of this article that the attorney general alleges have been or are being violated. If within the thirty (30) day period set forth in this section, the controller or processor:

(1) cures the alleged violation; and

(2) provides the attorney general an express written statement that:

(A) the alleged violation has been cured; and

(B) actions have been taken to ensure no further such violations will occur; the attorney general shall not initiate an action against the controller or processor.

(b) If a controller or processor:

(1) continues the alleged violation following the thirty (30) day period set forth in subsection (a); or

(2) breaches an express written statement provided to the attorney general under subsection (a)(2); the attorney general may initiate an action under section 2 of this chapter.

Sec. 4. Nothing in this article shall be construed as providing the basis for a private right of action for violations of this article or any other law.

Chapter 11. Preemption; Other Laws

Sec. 1. This article supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the processing of personal data by controllers or processors.

Sec. 2. Any reference to federal, state, or local law or statute in this article includes any accompanying rules, regulations, or exemptions.

SECTION 2. [EFFECTIVE UPON PASSAGE] (a) As used in this SECTION, "controller" has the meaning set forth in IC 24-15-2-9, as added by this act.

(b) The attorney general may, not later than December 31, 2025, establish on the attorney general's website a list of resources for controllers, including sample privacy notices and disclosures, to assist controllers in complying with IC 24-15-4, as added by this act.

(c) This SECTION expires July 1, 2026.

SECTION 3. An emergency is declared for this act.

Iowa Relating To Consumer Data Protection, Providing Civil Penalties, and Including Effective Date Provisions

AN ACT RELATING TO CONSUMER DATA PROTECTION, PROVIDING CIVIL PENALTIES, AND INCLUDING EFFECTIVE DATE PROVISIONS. BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:

Sec. 1. NEW SECTION. 715D.1 Definitions.

As used in this chapter, unless the context otherwise requires:

1. "Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity or shares common branding with another legal entity. For the purposes of this definition, "control" or "controlled" means:

   a. Ownership of, or the power to vote, more than fifty percent of the outstanding shares of any class of voting security of a company.

   b. Control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

   c. The power to exercise controlling influence over the management of a company.

2. "Aggregate data" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer.

3. "Authenticate" means verifying through reasonable means that a consumer, entitled to exercise their consumer rights in section 715D.3, is the same consumer exercising such consumer rights with respect to the personal data at issue.

4. "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. -Biometric data does not include a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment or operations under HIPAA.

5. "Child" means any natural person younger than thirteen years of age.

6. "Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. "Consent" may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action.

7. "Consumer" means a natural person who is a resident of the state acting only in an individual or household context and excluding a natural person acting in a commercial or employment context.

8. "Controller" means a person that, alone or jointly with others, determines the purpose and means of processing personal data.

9. "Covered entity" means the same as "covered entity" defined by HIPAA.

10. "De-identified data" means data that cannot reasonably be linked to an identified or identifiable natural person.

11. "Fund" means the consumer education and litigation fund established pursuant to section 714.16C.

12. "Health care provider" means any of the following:

    a. A general hospital, ambulatory surgical or treatment center, skilled nursing center, or assisted living center licensed or certified by the state.

    b. A psychiatric hospital licensed by the state.

c. A hospital operated by the state.

d. A hospital operated by the state board of regents.

e. A person licensed to practice medicine or osteopathy in the state.

f. A person licensed to furnish health care policies or plans in the state.

g. A person licensed to practice dentistry in the state.

h. Health care provider - does not include a continuing care retirement community or any nursing facility of a religious body which depends upon prayer alone for healing.

13. "Health Insurance Portability and Accountability Act" or "HIPAA" means the federal Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, including amendments thereto and regulations promulgated thereunder.

14. Health record means any written, printed, or electronically recorded material maintained by a health care provider in the course of providing health services to an individual concerning the individual and the services provided, including related health information provided in confidence to a health care provider.

15. "Identified or identifiable natural person" means a person who can be readily identified, directly or indirectly.

16. "Institution of higher education" means nonprofit private institutions of higher education and proprietary private institutions of higher education in the state, community colleges, and each associate "degree" granting and baccalaureate public institutions of higher education in the state.

17. "Nonprofit organization" means any corporation organized under chapter 504, any organization exempt from taxation under sections 501(c)(3), 501(c)(6), or 501(c)(12) of the Internal Revenue Code, any organization exempt from taxation under section 501(c)(4) of the Internal Revenue Code that is established to detect or prevent insurance-related crime or fraud, and any subsidiaries and affiliates of entities organized pursuant to chapter 499.

18. "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal data" does not include de-identified or aggregate data or publicly available information.

19. "Precise geolocation data" means information derived from technology, including but not limited to global positioning system level latitude and longitude coordinates or other mechanisms, that identifies the specific location of a natural person with precision and accuracy within a radius of one thousand seven hundred fifty feet. "Precise geolocation data" does not include the content of communications, or any data generated by or connected to utility metering infrastructure systems or equipment for use by a utility.

20. "Process" or "processing" means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

21. "Processor" means a person that processes personal data on behalf of a controller.

22. "Protected health information" means the same as protected health information established by HIPAA.

23. "Pseudonymous data" means personal data that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

24. "Publicly available information" means information that is lawfully made available through federal, state, or local government records, or information that a business has reasonable basis to believe is lawfully made available to the

general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.

25. "Sale of personal data" means the exchange of personal data for monetary consideration by the controller to a third party. "Sale of personal data" does not include:

    a. The disclosure of personal data to a processor that processes the personal data on behalf of the controller.

    b. The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer or a parent of a child.

    c. The disclosure or transfer of personal data to an affiliate of the controller.

    d. The disclosure of information that the consumer intentionally made available to the general public via a channel of mass media and did not restrict to a specific audience.

    e. The disclosure or transfer of personal data when a consumer uses or directs a controller to intentionally disclose personal data or intentionally interact with one or more third parties.

    f. The disclosure or transfer of personal data to a third party as an asset that is part of a proposed or actual merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

26. "Sensitive data" means a category of personal data that includes the following:

    a. Racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status, except to the extent such data is used in order to avoid discrimination on the basis of a protected class that would violate a federal or state anti-discrimination law.

    b. Genetic or biometric data that is processed for the purpose of uniquely identifying a natural person.

    c. The personal data collected from a known child. d. Precise geolocation data.

27. "State agency" means the same as defined in 129 IAC 10.2(8B).

28. "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests. "Targeted advertising" does not include the following:

    a. Advertisements based on activities within a controller's own or affiliated websites or online applications.

    b. Advertisements based on the context of a consumer's current search query, visit to a website, or online application.

    c. Advertisements directed to a consumer in response to the consumer's request for information or feedback.

    d. Processing personal data solely for measuring or reporting advertising performance, reach, or frequency.

29. "Third party" means a natural or legal person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller.

30. "Trade secret" means information, including but not limited to a formula, pattern, compilation, program, device, method, technique, or process, that consists of the following: a. Information that derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use. b. Information that is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Sec. 2. NEW SECTION. 715D.2 Scope and exemptions.

1. This chapter applies to a person conducting business in the state or producing products or services that are targeted to consumers who are residents of the state and that during a calendar year does either of the following:

   a. Controls or processes personal data of at least one hundred thousand consumers.

   b. Controls or processes personal data of at least twenty-five thousand consumers and derives over fifty percent of gross revenue from the sale of personal data.

2. This chapter shall not apply to the state or any political subdivision of the state; financial institutions, affiliates of financial institutions, or data subject to Tit. V of the federal Gramm-Leach- Bliley Act of 1999, 15 U.S.C. § 6801 et seq.; persons who are subject to and comply with regulations promulgated pursuant to Tit. II, subtit. F, of the federal Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, and Tit. XIII, subtit. D, of the federal Health Information Technology for Economic and Clinical Health Act of 2009, 42 U.S.C. § 17921 - 17954; nonprofit organizations; or institutions of higher education.

3. The following information and data is exempt from this chapter:

   a. Protected health information under HIPAA.

   b. Health records.

   c. Patient identifying information for purposes of 42 U.S.C. §290dd-2.

   d. Identifiable private information for purposes of the federal policy for the protection of human subjects under 45 C.F.R. pt. 46.

   e. Identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the international council for harmonization of technical requirements for pharmaceuticals for human use.

   f. The protection of human subjects under 21 C.F.R. pts. 6, 50, and 56.

   g. Personal data used or shared in research conducted in accordance with the requirements set forth in this chapter, or other research conducted in accordance with applicable law.

   h. Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, 42 U.S.C. §11101 et seq.

   i. Patient safety work product for purposes of the federal Patient Safety and Quality Improvement Act, 42 U.S.C. § 299b-21 et seq.

   j. Information derived from any of the health care- related information listed in this subsection that is de- identified in accordance with the requirements for de- identification pursuant to HIPAA.

   k. Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as information exempt under this subsection that is maintained by a covered entity or business associate as defined by HIPAA or a program or a qualified service organization as defined by 42 U.S.C. § 290dd-2.

   l. Information used only for public health activities and purposes as authorized by HIPAA.

   m. The collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency or furnisher that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the federal Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq.

   n. Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 et seq.

o. Personal data regulated by the federal Family Educational Rights and Privacy Act, 20 U.S.C. § 1232 et seq.

p. Personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act, 12 U.S.C. § 2001 et seq.

q. Data processed or maintained as follows:

(1) In the course of an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role.

(2) As the emergency contact information of an individual under this chapter used for emergency contact purposes.

(3) That is necessary to retain to administer benefits for another individual relating to the individual under subparagraph (1) and used for the purposes of administering those benefits.

r. Personal data used in accordance with the federal Children's Online Privacy Protection Act, 15 U.S.C. § 6501 — 6506, and its rules, regulations, and exceptions thereto.

Sec. 3. NEW SECTION. 715D.3 Consumer data rights.

1. A consumer may invoke the consumer rights authorized pursuant to this section at any time by submitting a request to the controller, through the means specified by the controller pursuant to section 715D.4, subsection 6, specifying the consumer rights the consumer wishes to invoke. A known child's parent or legal guardian may invoke such consumer rights on behalf of the known child regarding processing personal data belonging to the child. A controller shall comply with an authenticated consumer request to exercise all of the Senate File 262, p. 9 following:

a. To confirm whether a controller is processing the consumer's personal data and to access such personal data.

b. To delete personal data provided by the consumer.

c. To obtain a copy of the consumer's personal data, except as to personal data that is defined as personal information pursuant to section 715C.1 that is subject to security breach protection, that the consumer previously provided to the controller in a portable and, to the extent technically practicable, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means. d. To opt out of the sale of personal data.

2. Except as otherwise provided in this chapter, a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to this section as follows:

a. A controller shall respond to the consumer without undue delay, but in all cases within ninety days of receipt of a request submitted pursuant to the methods described in this section. The response period may be extended once by forty-five additional days when reasonably necessary upon considering the complexity and number of the consumer's requests by informing the consumer of any such extension within the initial ninety- day response period, together with the reason for the extension.

b, If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay of the justification for declining to take action, except in the case of a suspected fraudulent request, in which case the controller may state that the controller was unable to authenticate the request. The controller shall also provide instructions for appealing the decision pursuant to subsection 3.

c. Information provided in response to a consumer request shall be provided by a controller free of charge, up to twice annually per consumer. If a request from a consumer is manifestly unfounded, excessive, repetitive, technically unfeasible, or the controller reasonably believes that the primary purpose of the request is not to exercise a consumer right, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive, repetitive, or technically unfeasible nature of the request.

d. If a controller is unable to authenticate a request using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action under this section and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.

3. A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision pursuant to this section. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Within sixty days of receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decision. If the appeal is denied, the controller shall also provide the consumer with an online mechanism through which the consumer may contact the attorney general to submit a complaint.

Sec. 4. NEW SECTION. 715D.4 Data controller duties.

1. A controller shall adopt and implement reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue.

2. A controller shall not process sensitive data collected from a consumer for a nonexempt purpose without the consumer having been presented with clear notice and an opportunity to opt out of such processing, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with the federal Children's Online Privacy Protection Act, 15 U.S.C. § 6501 et seq.

3. A controller shall not process personal data in violation of state and federal laws that prohibit unlawful discrimination against a consumer. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer. However, nothing in this chapter shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised the consumer's right to opt out pursuant to section 715D.3 or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

4. Any provision of a contract or agreement that purports to waive or limit in any way consumer rights pursuant to section 715D.3 shall be deemed contrary to public policy and shall be void and unenforceable.

5. A controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes the following:

   a. The categories of personal data processed by the controller.

   b. The purpose for processing personal data.

   c. How consumers may exercise their consumer rights pursuant to section 715D.3, including how a consumer may appeal a controller's decision with regard to the consumer's request.

   d. The categories of personal data that the controller shares with third parties, if any.

   e. The categories of third parties, if any, with whom the controller shares personal data.

6. If a controller sells a consumer's personal data to third parties or engages in targeted advertising, the controller shall clearly and conspicuously disclose such activity, as well as the manner in which a consumer may exercise the right to opt out of such activity.

7. A controller shall establish, and shall describe in a privacy notice, secure and reliable means for consumers to submit a request to exercise their consumer rights under this chapter. Such means shall consider the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests, and the ability of the controller to authenticate the identity of the consumer making the request. A controller shall not require a consumer to create a new account in order to exercise consumer rights pursuant to section 715D.3, but may require a consumer to use an existing account.

Sec. 5. NEW SECTION. 715D.5 Processor duties.

1. A processor shall assist a controller in duties required under this chapter, taking into account the nature of processing and the information available to the processor by appropriate technical and organizational measures, insofar as is reasonably practicable, as follows:

   a. To fulfill the controller's obligation to respond to consumer rights requests pursuant to section 715D.3.

   b. To meet the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a security breach of the processor pursuant to section 715C.2.

2. A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall clearly set forth instructions for processing personal data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and duties of both parties. The contract shall also include requirements that the processor shall do all of the following:

   a. Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data.

   b. At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law.

   c. Upon the reasonable request of the controller, make available to the controller all information in the processor's possession necessary to demonstrate the processor's compliance with the obligations in this chapter.

   d. Engage any subcontractor or agent pursuant to a written contract in accordance with this section that requires the subcontractor to meet the duties of the processor with respect to the personal data.

3. Nothing in this section shall be construed to relieve a controller or a processor from imposed liabilities by virtue of the controller or processor's role in the processing relationship as defined by this chapter.

4. Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor.

Sec. 6. NEW SECTION. 715D.6 Processing data — exemptions.

1. Nothing in this chapter shall be construed to require the following:

   a. A controller or processor to re- identify de- identified data or pseudonymous data.

   b. Maintaining data in identifiable form.

   c. Collecting, obtaining, retaining, or accessing any data or technology, in order to be capable of associating an authenticated consumer request with personal data.

2. Nothing in this chapter shall be construed to require a controller or processor to comply with an authenticated consumer rights request, pursuant to section 715D.3, if all of the following apply:

   a. The controller is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data.

   b. The controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer.

   c. The controller does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this chapter.

3. Consumer rights contained in sections 715D.3 and 715D.4 shall not apply to pseudonymous data in cases where the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

4. Controllers that disclose pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

Sec. 7. NEW SECTION. 715D.7 Limitations.

1. Nothing in this chapter shall be construed to restrict a controller's or processor's ability to do the following:

   a. Comply with federal, state, or local laws, rules, or regulations.

   b. Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities.

   c. Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations.

   d. Investigate, establish, exercise, prepare for, or defend legal claims.

   e. Provide a product or service specifically requested by a consumer or parent or guardian of a child, perform a contract to which the consumer or parent or guardian of a child is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer or parent or guardian of a child prior to entering into a contract.

   f. Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis.

   g, Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity.

   h. Preserve the integrity or security of systems.

   i. Investigate, report, or prosecute those responsible for any such action.

   j. Engage in public or peer- reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, or similar independent oversight entities that determine the following:

      (1) If the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller.

      (2) The expected benefits of the research outweigh the privacy risks.

      (3) If the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re- identification.

k. Assist another controller, processor, or third party with any of the obligations under this subsection. 2. The obligations imposed on a controller or processor under this chapter shall not restrict a controller's or processor's ability to collect, use, or retain data as follows: a. To conduct internal research to develop, repair products, services, or technology. b. To effectuate a product recall. c. To identify and repair technical errors existing or intended functionality. d. To perform internal operations that are improve, or that impair reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or parent or guardian of a child or the performance of a contract to which the consumer or Senate File 262, p. 16 parent or guardian of a child is a party.

3. The obligations imposed on controllers or processors under this chapter shall not apply where compliance by the controller or processor with this chapter would violate an evidentiary privilege under the laws of the state. Nothing in this chapter shall be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of the state as part of a privileged communication.

4. A controller or processor that discloses personal data to a third-party controller or processor, in compliance with the requirements of this chapter, is not in violation of this chapter if the third-party controller or processor that receives and processes such personal data is in violation of this chapter, provided that, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation. A third-party controller or processor receiving personal data from a controller or processor in compliance with the requirements of this chapter is likewise not in violation of this chapter for the offenses of the controller or processor from which it receives such personal data.

5. Nothing in this chapter shall be construed as an obligation imposed on a controller or a processor that adversely affects the privacy or other rights or freedoms of any persons, such as exercising the right of free speech pursuant to the first amendment to the United States Constitution, or applies to personal data by a person in the course of a purely personal or household activity.

6. Personal data processed by a controller pursuant to this section shall not be processed for any purpose other than those expressly listed in this section unless otherwise allowed by this chapter. Personal data processed by a controller pursuant to this section may be processed to the extent that such processing is as follows:

   a. Reasonably necessary and proportionate to the purposes listed in this section.

   b. Adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section. Personal data collected, used, or retained pursuant to this section shall, where applicable, take into account the nature and purpose or purposes of such collection, use, or retention. Such data shall be subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data.

7. If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in subsection 6.

8. Processing personal data for the purposes expressly identified in subsection 1 shall not in and of itself make an entity a controller with respect to such processing.

9. This chapter shall not require a controller, processor, third party, or consumer to disclose trade secrets.

Sec. 8. NEW SECTION. 715D.8 Enforcement — penalties.

1. The attorney general shall have exclusive authority to enforce the provisions of this chapter. Whenever the attorney general has reasonable cause to believe that any person has engaged in, is engaging in, or is about to engage in any violation of this chapter, the attorney general is empowered to issue a civil investigative demand. The provisions of section 685.6 shall apply to civil investigative demands issued under this chapter.

2. Prior to initiating any action under this chapter, the attorney general shall provide a controller or processor ninety days" written notice identifying the specific provisions of this chapter the attorney general alleges have been or are being violated. If within the ninety- day period, the controller or processor cures the noticed violation and provides the attorney general an express written statement that the alleged violations have been cured and that no further such violations shall occur, no action shall be initiated against the controller or processor.

3. If a controller or processor continues to violate this chapter following the cure period in subsection 2 or breaches an express written statement provided to the attorney general under that subsection, the attorney general may initiate an action in the name of the state and may seek an injunction to restrain any violations of this chapter and civil penalties of up to seven thousand five hundred dollars for each violation under this chapter. Any moneys collected under this section including civil penalties, costs, attorney fees, or amounts which are specifically directed shall be paid into the consumer education and litigation fund established under section 714.16C.

4. Nothing in this chapter shall be construed as providing the basis for, or be subject to, a private right of action for violations of this chapter or under any other law.

Sec. 9. NEW SECTION. 715D.9 Preemption.

1. This chapter supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, municipality, or local agency regarding the processing of personal data by controllers or processors. 2. Any reference to federal, state, or local law or statute in this chapter shall be deemed to include any accompanying rules or regulations or exemptions thereto, or in the case of a federal agency, guidance issued by such agency thereto.

Sec. 10. EFFECTIVE DATE. This Act takes effect January 1, 2025.

Florida Technology Transparency

Section 4. Section 501.701, Florida Statutes, is created to read:

501.701 Short title.

This part may be cited as the "Florida Digital Bill of Rights."

Section 5. Section 501.702, Florida Statutes, is created to read:

501.702 Definitions.

As used in this part, the term:

(1) "Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity or that shares common branding with another legal entity. For purposes of this subsection, the term "control" or "controlled" means any of the following:

(a) The ownership of, or power to vote, more than 50 percent of the outstanding shares of any class of voting security of a company.

(b) The control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(c) The power to exercise controlling influence over the management of a company.

(2) "Aggregate consumer information" means information that relates to a group or category of consumers, from which the identity of an individual consumer has been removed and is not reasonably capable of being directly or indirectly associated or linked with any consumer, household, or device. The term does not include information about a group or category of consumers used to facilitate targeted advertising or the display of ads online. The term does not include personal information that has been deidentified.

(3) "Authenticate" or "authenticated" means to verify or the state of having been verified, respectively, through reasonable means that the consumer who is entitled to exercise the consumer's rights under s. 501.705 is the same consumer exercising those consumer rights with respect to the personal data at issue.

(4) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics. The term includes fingerprints, voiceprints, eye retinas or irises, or other unique biological patterns or characteristics used to identify a specific individual. The term does not include physical or digital photographs, video or audio recordings or data generated from video or audio recordings, or information collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.

(5) "Business associate" has the same meaning as in 45 C.F.R. s. 160.103 and the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.

(6) "Child" means an individual younger than 18 years of age.

(7) "Consent," when referring to a consumer, means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. The term includes a written statement, including a statement written by electronic means, or any other unambiguous affirmative act. The term does not include any of the following:

(a) Acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information.

(b) Hovering over, muting, pausing, or closing a given piece of content.

(c) Agreement obtained through the use of dark patterns.

(8) "Consumer" means an individual who is a resident of or is domiciled in this state acting only in an individual or household context. The term does not include an individual acting in a commercial or employment context.

(9) "Controller" means:

(a) A sole proprietorship, partnership, limited liability company, corporation, association, or legal entity that meets the following requirements:

1. Is organized or operated for the profit or financial benefit of its shareholders or owners;
2. Conducts business in this state;
3. Collects personal data about consumers, or is the entity on behalf of which such information is collected;
4. Determines the purposes and means of processing personal data about consumers alone or jointly with others;
5. Makes in excess of $1 billion in global gross annual revenues; and
6. Satisfies at least one of the following:

a. Derives 50 percent or more of its global gross annual revenues from the sale of advertisements online, including providing targeted advertising or the sale of ads online;

b. Operates a consumer smart speaker and voice command component service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation. For purposes of this sub-subparagraph, a consumer smart speaker and voice command component service does not include a motor vehicle or speaker or device associated with or connected to a vehicle which is operated by a motor vehicle manufacturer or a subsidiary or affiliate thereof; or

c. Operates an app store or a digital distribution platform that offers at least 250,000 different software applications for consumers to download and install.

(b) Any entity that controls or is controlled by a controller. As used in this paragraph, the term "control" means:

1. Ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a controller;
2. Control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or
3. The power to exercise a controlling influence over the management of a company.

(10) "Covered entity" has the same meaning as in 45 C.F.R. s. 160.103 and the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.

(11) "Dark pattern" means a user interface designed or manipulated with the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice. The term includes any practice the Federal Trade Commission refers to as a dark pattern.

(12) "Decision that produces a legal or similarly significant effect concerning a consumer" means a decision made by a controller which results in the provision or denial by the controller of any of the following:

(a) Financial and lending services.

(b) Housing, insurance, or health care services.

(c) Education enrollment.

(d) Employment opportunities.

(e) Criminal justice.

(f) Access to basic necessities, such as food and water.

(13) "Deidentified data" means data that cannot reasonably be linked to an identified or identifiable individual or a device linked to that individual.

(14) "Health care provider" has the same meaning as in 45 C.F.R. s. 160.103 and the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.

(15) "Health record" means any written, printed, or electronically recorded material maintained by a health care provider in the course of providing health care services to an individual which concerns the individual and the services provided. The term includes any of the following:

(a) The substance of any communication made by an individual to a health care provider in confidence during or in connection with the provision of health care services.

(b) Information otherwise acquired by the health care provider about an individual in confidence and in connection with health care services provided to the individual.

(16) "Identified or identifiable individual" means a consumer who can be readily identified, directly or indirectly.

(17) "Known child" means a child under circumstances of which a controller has actual knowledge of, or willfully disregards, the child's age.

(18) "Nonprofit organization" means any of the following:

(a) An organization exempt from federal taxation under s. 501(a) of the Internal Revenue Code of 1986 by virtue of being listed as an exempt organization under s. 501(c)(3), s. 501(c)(4), s. 501(c)(6), or s. 501(c)(12) of that code.

(b) A political organization.

(19) "Personal data" means any information, including sensitive data, which is linked or reasonably linkable to an identified or identifiable individual. The term includes pseudonymous data when the data is used by a controller or processor in conjunction with additional information that reasonably links the data to an identified or identifiable individual. The term does not include deidentified data or publicly available information.

(20) "Political organization" means a party, a committee, an association, a fund, or any other organization, regardless of whether incorporated, organized and operated primarily for the purpose of influencing or attempting to influence any of the following:

(a) The selection, nomination, election, or appointment of an individual to a federal, state, or local public office or an office in a political organization, regardless of whether the individual is selected, nominated, elected, or appointed.

(b) The election of a presidential or vice-presidential elector, regardless of whether the elector is selected, nominated, elected, or appointed.

(21) "Postsecondary education institution" means a Florida College System institution, state university, or nonpublic postsecondary education institution that receives state funds.

(22) "Precise geolocation data" means information derived from technology, including global positioning system level latitude and longitude coordinates or other mechanisms, which directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet. The term does not include the content of communications or any data generated by or connected to an advanced utility metering infrastructure system or to equipment for use by a utility.

(23) "Process" or "processing" means an operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(24) "Processor" means a person who processes personal data on behalf of a controller.

(25) "Profiling" means any form of solely automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(26) "Protected health information" has the same meaning as in 45 C.F.R. s. 160.103 and the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.

(27) "Pseudonymous data" means any information that cannot be attributed to a specific individual without the use of additional information, provided that the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

(28) "Publicly available information" means information lawfully made available through government records, or information that a business has a reasonable basis for believing is lawfully made available to the general public through widely distributed media, by a consumer, or by a person to whom a consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.

(29) "Sale of personal data" means the sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party. The term does not include any of the following:

(a) The disclosure of personal data to a processor who processes the personal data on the controller's behalf.

(b) The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer.

(c) The disclosure of information that the consumer:

1. Intentionally made available to the general public through a mass media channel; and

2. Did not restrict to a specific audience.

(d) The disclosure or transfer of personal data to a third party as an asset that is part of a merger or an acquisition.

(30) "Search engine" means technology and systems that use algorithms to sift through and index vast third-party websites and content on the Internet in response to search queries entered by a user. The term does not include the license of search functionality for the purpose of enabling the licensee to operate a third-party search engine service in circumstances where the licensee does not have legal or operational control of the search algorithm, the index from which results are generated, or the ranking order in which the results are provided.

(31) "Sensitive data" means a category of personal data which includes any of the following:

(a) Personal data revealing an individual's racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status.

(b) Genetic or biometric data processed for the purpose of uniquely identifying an individual.

(c) Personal data collected from a known child.

(d) Precise geolocation data.

(32) "State agency" means any department, commission, board, office, council, authority, or other agency in the executive branch of state government created by the State Constitution or state law. The term includes a postsecondary education institution.

(33) "Targeted advertising" means displaying to a consumer an advertisement selected based on personal data obtained from that consumer's activities over time across affiliated or unaffiliated websites and online applications used to predict the consumer's preferences or interests. The term does not include an advertisement that is:

(a) Based on the context of a consumer's current search query on the controller's own website or online application; or

(b) Directed to a consumer search query on the controller's own website or online application in response to the consumer's request for information or feedback.

(34) "Third party" means a person, other than the consumer, the controller, the processor, or an affiliate of the controller or processor.

(35) "Trade secret" has the same meaning as in s. 812.081.

(36) "Voice recognition feature" means the function of a device which enables the collection, recording, storage, analysis, transmission, interpretation, or other use of spoken words or other sounds.

Section 6. Section 501.703, Florida Statutes, is created to read:

501.703 Applicability.

(1) This part applies only to a person who:

(a) Conducts business in this state or produces a product or service used by residents of this state; and

(b) Processes or engages in the sale of personal data.

(2) This part does not apply to any of the following:

(a) A state agency or a political subdivision of the state.

(b) A financial institution or data subject to Title V, Gramm-Leach-Bliley Act, 15 U.S.C. ss. 6801 et seq.

(c) A covered entity or business associate governed by the privacy, security, and breach notification regulations issued by the United States Department of Health and Human Services, 45 C.F.R. parts 160 and 164, established under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq., and the Health Information Technology for Economic and Clinical Health Act, Division A, Title XIII and Division B, Title IV, Pub. L. No. 111-5.

(d) A nonprofit organization.

(e) A postsecondary education institution.

(f) The processing of personal data:

1. By a person in the course of a purely personal or household activity.

2. Solely for measuring or reporting advertising performance, reach, or frequency.

(3) A controller or processor that complies with the authenticated parental consent requirements of the Children's Online Privacy Protection Act, 15 U.S.C. ss. 6501 et seq., with respect to data collected online, is considered to be in compliance with any requirement to obtain parental consent under this part.

Section 7. Section 501.704, Florida Statutes, is created to read:

501.704 Exemptions.

All of the following information is exempt from this part:

(1) Protected health information under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.

(2) Health records.

(3) Patient identifying information for purposes of 42 U.S.C. s. 290dd-2.

(4) Identifiable private information:

(a) For purposes of the federal policy for the protection of human subjects under 45 C.F.R. part 46;

(b) Collected as part of human subjects research under the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use or the protection of human subjects under 21 C.F.R. parts 50 and 56; or

(c) That is personal data used or shared in research conducted in accordance with this part or other research conducted in accordance with applicable law.

(5) Information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 U.S.C. ss. 11101 et seq.

(6) Patient safety work product for purposes of the Patient Safety and Quality Improvement Act of 2005, 42 U.S.C. ss. 299b 21 et seq.

(7) Information derived from any of the health-care-related information listed in this section which is deidentified in accordance with the requirements for deidentification under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.

(8) Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this section which is maintained by a covered entity or business associate as defined by the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq. or by a program or a qualified service organization as defined by 42 U.S.C. s. 290dd-2.

(9) Information included in a limited data set as described by 45 C.F.R. s. 164.514(e), to the extent that the information is used, disclosed, and maintained in the manner specified by 45 C.F.R. s. 164.514(e).

(10) Information used only for public health activities and purposes as described in 45 C.F.R. s. 164.512.

(11) Information collected or used only for public health activities and purposes as authorized by the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.

(12) The collection, maintenance, disclosure, sale, communication, or use of any personal data bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency or furnisher that provides information for use in a consumer report, or by a user of a consumer report, but only to the extent that the activity is regulated by and authorized under the Fair Credit Reporting Act, 15 U.S.C. ss. 1681 et seq.

(13) Personal data collected, processed, sold, or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 U.S.C. ss. 2721 et seq.

(14) Personal data regulated by the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. s. 1232g.

(15) Personal data collected, processed, sold, or disclosed in compliance with the Farm Credit Act of 1971, 12 U.S.C. ss. 2001 et seq.

(16) Data processed or maintained in the course of an individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role.

(17) Data processed or maintained as the emergency contact information of an individual under this part which is used for emergency contact purposes.

(18) Data that is processed or maintained and that is necessary to retain to administer benefits for another individual which relates to an individual described in subsection (16) and which is used for the purposes of administering those benefits.

(19) Personal data collected and transmitted which is necessary for the sole purpose of sharing such personal data with a financial service provider solely to facilitate short term, transactional payment processing for the purchase of products or services.

(20) Personal data collected, processed, sold, or disclosed in relation to price, route, or service as those terms are used in the Airline Deregulation Act, 49 U.S.C. ss. 40101 et seq., by entities subject to that act, to the extent the provisions of this act are preempted by 49 U.S.C. s. 41713.

(21) Personal data shared between a manufacturer of a tangible product and authorized third-party distributors or vendors of the product, as long as such personal data is used solely for advertising, marketing, or servicing the product that is acquired directly through such manufacturer and such authorized third-party distributors or vendors. Such personal data may not be sold or shared unless otherwise authorized under this part.

Section 8. Section 501.705, Florida Statutes, is created to read:

501.705 Consumer rights.

(1) A consumer is entitled to exercise the consumer rights authorized by this section at any time by submitting a request to a controller which specifies the consumer rights that the consumer wishes to exercise. With respect to the processing of personal data belonging to a known child, a parent or legal guardian of the child may exercise these rights on behalf of the child.

(2) A controller shall comply with an authenticated consumer request to exercise any of the following rights:

(a) To confirm whether a controller is processing the consumer's personal data and to access the personal data.

(b) To correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.

(c) To delete any or all personal data provided by or obtained about the consumer.

(d) To obtain a copy of the consumer's personal data in a portable and, to the extent technically feasible, readily usable format if the data is available in a digital format.

(e) To opt out of the processing of the personal data for purposes of:

1. Targeted advertising;

2. The sale of personal data; or

3. Profiling in furtherance of a decision that produces a legal or similarly significant effect concerning a consumer.

(f) To opt out of the collection of sensitive data, including precise geolocation data, or the processing of sensitive data.

(g) To opt out of the collection of personal data collected through the operation of a voice recognition or facial recognition feature.

(3) A device that has a voice recognition feature, a facial recognition feature, a video recording feature, an audio recording feature, or any other electronic, visual, thermal, or olfactory feature that collects data may not use those features for the purpose of surveillance by the controller, processor, or affiliate of a controller or processor when such features are not in active use by the consumer, unless otherwise expressly authorized by the consumer.

Section 9. Section 501.706, Florida Statutes, is created to read:

501.706 Controller response to consumer requests.

(1) Except as otherwise provided by this part, a controller shall comply with a request submitted by a consumer to exercise the consumer's rights pursuant to s. 501.705, as provided in this section.

(2) A controller shall respond to the consumer request without undue delay, which may not be later than 45 days after the date of receipt of the request. The controller may extend the response period once by an additional 15 days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of the extension within the initial 45-day response period, together with the reason for the extension.

(3) If a controller cannot take action regarding the consumer's request, the controller must inform the consumer without undue delay, which may not be later than 45 days after the date of receipt of the request, of the justification for the inability to take action on the request and provide instructions on how to appeal the decision in accordance with s. 501.707. A controller is not required to comply with a consumer request submitted under s. 501.705 if the controller cannot authenticate the request. However, the controller must make a reasonable effort to request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request. If a controller maintains a self service mechanism to allow a consumer to correct certain personal data, the controller may deny the consumer's request and require the consumer to correct his or her own personal data through such mechanism.

(4) A controller must provide the consumer with notice within 60 days after the request is received that the controller has complied with the consumer's request as required in this section.

(5) A controller shall provide information or take action in response to a consumer request free of charge, at least twice annually per consumer. If a request from a consumer is manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or may decline to act on the request. The controller bears the burden of demonstrating for purposes of this subsection that a request is manifestly unfounded, excessive, or repetitive.

(6) A controller who has obtained personal data about a consumer from a source other than the consumer is considered in compliance with a consumer's request to delete that personal data pursuant to s. 501.705(2)(c), by doing any of the following:

(a) Deleting the personal data, retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring that the consumer's personal data remains deleted from the business's records, and not using the retained data for any other purpose under this part.

(b) Opting the consumer out of the processing of that personal data for any purpose other than a purpose exempt under this part.

Section 10. Section 501.707, Florida Statutes, is created to read:

501.707 Appeal.

(1) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision under s. 501.706(3).

(2) The appeal process must be conspicuously available and similar to the process for initiating action to exercise consumer rights by submitting a request under s. 501.705.

(3) A controller shall inform the consumer in writing of any action taken or not taken in response to an appeal under this section within 60 days after the date of receipt of the appeal, including a written explanation of the reason or reasons for the decision.

Section 11. Section 501.708, Florida Statutes, is created to read:

501.708 Waiver or limitation of consumer rights prohibited.

Any provision of a contract or agreement which waives or limits in any way a consumer right described by s. 501.705, s. 501.706, or s. 501.707 is contrary to public policy and is void and unenforceable.

Section 12. Section 501.709, Florida Statutes, is created to read:

501.709 Submitting consumer requests.

(1) A controller shall establish two or more methods to enable consumers to submit a request to exercise their consumer rights under this part. The methods must be secure, reliable, and clearly and conspicuously accessible. The methods must take all of the following into account:

(a) The ways in which consumers normally interact with the controller.

(b) The necessity for secure and reliable communications of these requests.

(c) The ability of the controller to authenticate the identity of the consumer making the request.

(2) A controller may not require a consumer to create a new account to exercise the consumer's rights under this part but may require a consumer to use an existing account.

(3) A controller shall provide a mechanism on its website for a consumer to submit a request for information required to be disclosed under this part. A controller that operates exclusively online and has a direct relationship with a consumer from whom the controller collects personal data may also provide an e-mail address for the submission of requests.

Section 13. Section 501.71, Florida Statutes, is created to read:

501.71 Controller duties.

(1) A controller shall:

(a) Limit the collection of personal data to data that is adequate, relevant, and reasonably necessary in relation to the purposes for which it is processed, as disclosed to the consumer; and

(b) For purposes of protecting the confidentiality, integrity, and accessibility of personal data, establish, implement, and maintain reasonable administrative, technical, and physical data security practices appropriate to the volume and nature of the personal data at issue.

(2) A controller may not do any of the following:

(a) Except as otherwise provided by this part, process personal data for a purpose that is neither reasonably necessary nor compatible with the purpose for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.

(b) Process personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers.

(c) Discriminate against a consumer for exercising any of the consumer rights contained in this part, including by denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer. A controller may offer financial incentives, including payments to consumers as compensation, for processing of personal data if the consumer gives the controller prior consent that clearly describes the material terms of the financial incentive program and provided that such incentive practices are not unjust, unreasonable, coercive, or usurious in nature. The consent may be revoked by the consumer at any time.

(d) Process the sensitive data of a consumer without obtaining the consumer's consent, or, in the case of processing the sensitive data of a known child, without processing that data with the affirmative authorization for such processing by a known child who is between 13 and 18 years of age or in accordance with the Children's Online Privacy Protection Act, 15 960 U.S.C. ss. 6501 et seq. for a known child under the age of 13.

(3) Paragraph (2)(c) may not be construed to require a controller to provide a product or service that requires the personal data of a consumer which the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised the consumer's right to opt out under s. 501.705(2) or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

(4) A controller that operates a search engine shall make available, in an easily accessible location on the webpage which does not require a consumer to log in or register to read, an up-to-date plain language description of the main parameters that are individually or collectively the most significant in determining ranking and the relative importance of those main parameters, including the prioritization or deprioritization of political partisanship or political ideology in search results. Algorithms are not required to be disclosed nor is any other information that, with reasonable certainty, would enable deception of or harm to consumers through the manipulation of search results.

Section 14. Section 501.711, Florida Statutes, is created to read:

501.711 Privacy notices.

(1) A controller shall provide consumers with a reasonably accessible and clear privacy notice, updated at least annually, that includes all of the following information:

(a) The categories of personal data processed by the controller, including, if applicable, any sensitive data processed by the controller.

(b) The purpose of processing personal data.

(c) How consumers may exercise their rights under s. 501.705(2), including the process by which a consumer may appeal a controller's decision with regard to the consumer's request.

(d) If applicable, the categories of personal data that the controller shares with third parties.

(e) If applicable, the categories of third parties with whom the controller shares personal data.

(f) A description of the methods specified in s. 501.709, by which consumers can submit requests to exercise their consumer rights under this part.

(2) If a controller engages in the sale of personal data that is sensitive data, the controller must provide the following notice: "NOTICE: This website may sell your sensitive personal data." The notice must be posted in accordance with subsection (1).

(3) If a controller engages in the sale of personal data that is biometric data, the controller must provide the following notice: "NOTICE: This website may sell your biometric personal data." The notice must be posted in accordance with 1012 subsection (1).

(4) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller must clearly and conspicuously disclose that process and the manner in which a consumer may exercise the right to opt out of that process.

(5) A controller may not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

Section 15. Section 501.712, Florida Statutes, is created to read:

501.712 Duties of processor.

(1) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting or complying with the controller's duties under this section and the requirements of this part, including the following:

(a) Assisting the controller in responding to consumer rights requests submitted pursuant to ss. 501.705 and 501.709, by using appropriate technical and organizational measures, as reasonably practicable, taking into account the nature of processing and the information available to the processor.

(b) Assisting the controller with regard to complying with the requirement relating to the security of processing personal data and to the notification of a breach of security of the processor's system under s. 501.171, taking into account the nature of processing and the information available to the processor.

(c) Providing necessary information to enable the controller to conduct and document data protection assessments under s. 501.713.

(2) A contract between a controller and a processor governs the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract must include all of the following information:

(a) Clear instructions for processing data.

(b) The nature and purpose of processing.

(c) The type of data subject to processing.

(d) The duration of processing.

(e) The rights and obligations of both parties.

(f) A requirement that the processor:

1. Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

2. At the controller's direction, delete or return all personal data to the controller as requested after the provision of the service is completed, unless retention of the personal data is required by law;

3. Make available to the controller, upon reasonable request, all information in the processor's possession necessary to demonstrate the processor's compliance with this part;

4. Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; and

5. Engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the requirements of the processor with respect to the personal data.

(3) Notwithstanding subparagraph (2)(f)4., a processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the requirements under this part using an appropriate and accepted control standard or framework and assessment procedure. The processor shall provide a report of the assessment to the controller upon request.

(4) This section may not be construed to relieve a controller or a processor from the liabilities imposed on the controller or processor by virtue of its role in the processing relationship as described by this part.

(5) A determination as to whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends on the context in which personal data is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains in the role of a processor.

Section 16. Section 501.713, Florida Statutes, is created to read:

501.713 Data protection assessments.

(1) A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data:

(a) The processing of personal data for purposes of targeted advertising.

(b) The sale of personal data.

(c) The processing of personal data for purposes of profiling if the profiling presents a reasonably foreseeable risk of:

1. Unfair or deceptive treatment of or unlawful disparate impact on consumers;

2. Financial, physical, or reputational injury to consumers;

3. A physical or other intrusion on the solitude or seclusion, or the private affairs or concerns, of consumers, if the intrusion would be offensive to a reasonable person; or

4. Other substantial injury to consumers.

(d) The processing of sensitive data.

(e) Any processing activities involving personal data which present a heightened risk of harm to consumers.

(2) A data protection assessment conducted under subsection (1) must do all of the following:

(a) Identify and weigh the direct or indirect benefits that may flow from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with that processing, as mitigated by safeguards that can be employed by the controller to reduce such risks.

(b) Factor into the assessment:

1. The use of deidentified data;

2. The reasonable expectations of consumers;

3. The context of the processing; and

4. The relationship between the controller and the consumer whose personal data will be processed.

(3) The disclosure of a data protection assessment in compliance with a request from the Attorney General pursuant to s. 501.72 does not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

(4) A single data protection assessment may address a comparable set of processing operations which include similar activities.

(5) A data protection assessment conducted by a controller for the purpose of compliance with any other law or regulation may constitute compliance with the requirements of this section if the assessment has a reasonably comparable scope and effect.

(6) This section applies only to processing activities generated on or after July 1, 2023.

Section 17. Section 501.714, Florida Statutes, is created to read:

501.714 Deidentified data, pseudonymous data, and aggregate consumer information.

(1) A controller in possession of deidentified data shall do all of the following:

(a) Take reasonable measures to ensure that the data cannot be associated with an individual.

(b) Maintain and use the data in deidentified form. A controller may not attempt to reidentify the data, except that the controller may attempt to reidentify the data solely for the purpose of determining whether its deidentification processes satisfy the requirements of this section.

(c) Contractually obligate any recipient of the deidentified data to comply with this part.

(d) Implement business processes to prevent the inadvertent release of deidentified data.

(2) This part may not be construed to require a controller or processor to do any of the following:

(a) Reidentify deidentified data or pseudonymous data.

(b) Maintain data in an identifiable form or obtain, retain, or access any data or technology for the purpose of allowing the controller or processor to associate a consumer request with personal data.

(c) Comply with an authenticated consumer rights request under s. 501.705 if the controller:

1. Is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data;

2. Does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data or associate the personal data with other personal data about the same specific consumer; and

3. Does not sell the personal data to a third party or otherwise voluntarily disclose the personal data to a third party other than a processor, except as otherwise authorized by this section.

(3) The consumer rights enumerated under s. 501.705(2), and controller duties imposed under s. 501.71, do not apply to pseudonymous data or aggregate consumer information in cases in which the controller is able to demonstrate that any information necessary to identify the consumer is kept separate and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

(4) A controller that discloses pseudonymous data, deidentified data, or aggregate consumer information shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the data or information is subject and shall take appropriate steps to address any breach of the contractual commitments.

Section 18. Section 501.715, Florida Statutes, is created to read:

501.715 Requirements for sensitive data.—

(1) A person who meets the requirements of s. 501.702(9)(a)1., (a)2., and (a)3. for the definition of a controller may not engage in the sale of personal data that is sensitive data without receiving prior consent from the consumer or, if the sensitive data is of a known child, without processing that data with the affirmative authorization for such processing by a known child who is between 13 and 18 years of age or in accordance with the Children's Online Privacy Protection Act, 15 U.S.C. ss. 6501 et seq. for a known child under the age of 13.

(2) A person in subsection (1) who engages in the sale of personal data that is sensitive data must provide the following notice: "NOTICE: This website may sell your sensitive personal data."

(3) A person who violates this section is subject to the penalty imposed under s. 501.72.

Section 19. Section 501.716, Florida Statutes, is created to read:

501.716 Exemptions for certain uses of consumer personal data.

(1) This part may not be construed to restrict a controller's or processor's ability to do any of the following:

(a) Comply with federal or state laws, rules, or regulations.

(b) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities.

(c) Investigate, establish, exercise, prepare for, or defend legal claims.

(d) Provide a product or service specifically requested by a consumer or the parent or guardian of a child, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer before entering into a contract.

(e) Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another individual and in which the processing cannot be manifestly based on another legal basis.

(f) Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity.

(g) Preserve the integrity or security of systems or investigate, report, or prosecute those responsible for breaches of system security.

(h) Engage in public or peer-reviewed scientific or statistical research in the public interest which adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board or similar independent oversight entity that determines:

1. Whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller;

2. Whether the expected benefits of the research outweigh the privacy risks; and

3. Whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification.

(i) Assist another controller, processor, or third party in complying with the requirements of this part.

(j) Disclose personal data disclosed when a consumer uses or directs the controller to intentionally disclose information to a third party or uses the controller to intentionally interact with a third party. An intentional interaction occurs when the consumer intends to interact with the third party, by one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.

(k) Transfer personal data to a third party as an asset that is part of a merger, an acquisition, a bankruptcy, or other transaction in which the third party assumes control of all or part of the controller, provided that the information is used or shared in a manner consistent with this part. If a third party materially alters how it uses or shares the personal data of a consumer in a manner that is materially inconsistent with the commitments or promises made at the time of collection, it must provide prior notice of the new or changed practice to the consumer. The notice must be sufficiently prominent and robust to ensure that consumers can easily exercise choices consistent with this part.

(2) This part may not be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of this state as part of a privileged communication.

(3) This part may not be construed as imposing a requirement on controllers and processors which adversely affects the rights or freedoms of any person, including the right of free speech.

(4) This part may not be construed as requiring a controller, processor, third party, or consumer to disclose a trade secret.

Section 20. Section 501.717, Florida Statutes, is created to read:

501.717 Collection, use, or retention of data for certain purposes.

(1) The requirements imposed on controllers and processors under this part may not restrict a controller's or processor's ability to collect, use, or retain data to do any of the following:

(a) Conduct internal research to develop, improve, or repair products, services, or technology.

(b) Effect a product recall.

(c) Identify and repair technical errors that impair existing or intended functionality.

(d) Perform internal operations that are:

1. Reasonably aligned with the expectations of the consumer;

2. Reasonably anticipated based on the consumer's existing relationship with the controller; or

3. Otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

(2) A requirement imposed on a controller or processor under this part does not apply if compliance with the requirement by the controller or processor, as applicable, would violate an evidentiary privilege under the laws of this state.

Section 21. Section 501.718, Florida Statutes, is created to read:

501.718 Disclosure of personal data to third-party controller or processor.

(1) A controller or processor that discloses personal data to a third-party controller or processor in compliance with the requirements of this part does not violate this part if the third-party controller or processor that receives and processes that personal data violates this part, provided that, at the time of the data's disclosure, the disclosing controller or processor could not have reasonably known that the recipient intended to commit a violation.

(2) A third-party controller or processor receiving personal data from a controller or processor in compliance with the requirements of this part may not be held liable for violations of this part committed by the controller or processor from which the third-party controller or processor receives the personal data.

Section 22. Section 501.719, Florida Statutes, is created to read:

501.719 Processing of certain personal data by controller or other person.

(1) Personal data processed by a controller pursuant to ss. 501.716, 501.717, and 501.718 may not be processed for any purpose other than those specified in those sections. Personal data processed by a controller pursuant to ss. 501.716, 501.717, and 501.718 may be processed to the extent that the processing of the data is:

(a) Reasonably necessary and proportionate to the purposes specified in ss. 501.716, 501.717, and 501.718;

(b) Adequate, relevant, and limited to what is necessary in relation to the purposes specified in ss. 501.716, 501.717, and 501.718; and

(c) Done to assist another controller, processor, or third party with any of the purposes specified in s. 501.716, s. 501.717, or s. 501.718.

(2) A controller or processor that collects, uses, or retains personal data for the purposes specified in s. 501.717(1) must take into account the nature and purpose of such collection, use, or retention. Such personal data is subject to reasonable administrative, technical, and physical measures to protect its confidentiality, integrity, and accessibility and to reduce reasonably foreseeable risks of harm to consumers relating to the collection, use, or retention of personal data.

(3) A controller or processor shall adopt and implement a retention schedule that prohibits the use or retention of personal data not subject to an exemption by the controller or processor after the satisfaction of the initial purpose for which such information was collected or obtained, after the expiration or termination of the contract pursuant to which the information was collected or obtained, or 2 years after the consumer's last interaction with the controller or processor. This subsection does not apply to personal data reasonably used or retained to do any of the following:

(a) Provide a good or service requested by the consumer, or reasonably anticipate the request of such good or service within the context of a controller's ongoing business relationship with the consumer.

(b) Debug to identify and repair errors that impair existing intended functionality.

(c) Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the controller or that are compatible with the context in which the consumer provided the information.

(4) A controller or processor that processes personal data pursuant to ss. 501.716, 501.717, and 501.718 bears the burden of demonstrating that the processing of the personal data qualifies for the exemption and complies with the requirements of this section.

Section 23. Section 501.72, Florida Statutes, is created to read:

501.72 Enforcement and implementation by the Department of Legal Affairs.

(1) A violation of this part is an unfair and deceptive trade practice actionable under part II of this chapter solely by the Department of Legal Affairs. If the department has reason to believe that a person is in violation of this section, the department may, as the enforcing authority, bring an action against such person for an unfair or deceptive act or practice. For the purpose of bringing an action pursuant to this section, ss. 501.211 and 501.212 do not apply. In addition to other remedies under part II of this chapter, the department may collect a civil penalty of up to $50,000 per violation. Civil penalties may be tripled for any of the following violations:

(a) A violation involving a Florida consumer who is a known child. A controller that willfully disregards the consumer's age is deemed to have actual knowledge of the consumer's age.

(b) Failure to delete or correct the consumer's personal data pursuant to this section after receiving an authenticated consumer request or directions from a controller to delete or correct such personal data, unless an exception to the requirements to delete or correct such personal data under this section applies.

(c) Continuing to sell or share the consumer's personal data after the consumer chooses to opt out under this part.

(2) After the department has notified a person in writing of an alleged violation, the department may grant a 45-day period to cure the alleged violation and issue a letter of guidance. The 45-day cure period does not apply to an alleged violation of paragraph (1)(a). The department may consider the number and frequency of violations, the substantial likelihood of injury to the public, and the safety of persons or property in determining whether to grant 45 calendar days to cure and the issuance of a letter of guidance. If the alleged violation is cured to the satisfaction of the department and proof of such cure is provided to the department, the department may not bring an action for the alleged violation but in its discretion may issue a letter of guidance that indicates that the person will not be offered a 45-day cure period for any future violations. If the person fails to cure the alleged violation within 45 calendar days, the department may bring an action against such person for the alleged violation.

(3) Any action brought by the department may be brought only on behalf of a Florida consumer.

(4) By February 1 of each year, the department shall make a report publicly available on the department's website describing any actions taken by the department to enforce this section. The report must include statistics and relevant information detailing all of the following:

(a) The number of complaints received and the categories or types of violations alleged by the complainant.

(b) The number and type of enforcement actions taken and the outcomes of such actions, including the amount of penalties issued and collected.

(c) The number of complaints resolved without the need for litigation.

(d) For the report due February 1, 2024, the status of the development and implementation of rules to implement this section.

(5) The department shall adopt rules to implement this section, including standards for authenticated consumer requests, enforcement, data security, and authorized persons who may act on a consumer's behalf.

(6) The department may collaborate and cooperate with other enforcement authorities of the Federal Government or other state governments concerning consumer data privacy issues and consumer data privacy investigations if such enforcement authorities have restrictions governing confidentiality at least as stringent as the restrictions provided in this section.

(7) Liability for a tort, contract claim, or consumer protection claim unrelated to an action brought under this section does not arise solely from the failure of a person to comply with this part.

(8) This part does not establish a private cause of action.

(9) The department may employ or use the legal services of outside counsel and the investigative services of outside personnel to fulfill the obligations of this section.

(10) For purposes of bringing an action pursuant to this section, any person who meets the definition of controller as defined in this part who collects, shares, or sells the personal data of Florida consumers is considered to be engaged in both substantial and not isolated activities within this state and operating, conducting, engaging in, or carrying on a business, and doing business in this state, and is, therefore, subject to the jurisdiction of the courts of this state.

Section 24. Section 501.721, Florida Statutes, is created to read:

501.721 Preemption.

This part is a matter of statewide concern and supersedes all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection, processing, sharing, or sale of consumer personal data by a controller or processor. The regulation of the collection, processing, sharing, or sale of consumer personal data by a controller or processor is preempted to the state.

Section 25. Paragraph (g) of subsection (1) of section 501.171, Florida Statutes, is amended to read:

501.171 Security of confidential personal information.

(1) DEFINITIONS.—As used in this section, the term:

(g)1. "Personal information" means either of the following:

a. An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:

(I) A social security number;

(II) A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;

(III) A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;

(IV) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;

(V) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual;

(VI) An individual's biometric data as defined in s. 501.702; or

(VII) Any information regarding an individual's geolocation.

b. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

2. The term does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

Section 26. Subsection (1) of section 16.53, Florida Statutes, is amended, and subsection (8) is added to that section, to read:

16.53 Legal Affairs Revolving Trust Fund.

(1) There is created in the State Treasury the Legal Affairs Revolving Trust Fund, from which the Legislature may appropriate funds for the purpose of funding investigation, prosecution, and enforcement by the Attorney General of the provisions of the Racketeer Influenced and Corrupt Organization Act, the Florida Deceptive and Unfair Trade Practices Act, the Florida False Claims Act, state or federal antitrust laws, s. 501.1735, or part V of chapter 501. (8) All moneys recovered by the Attorney General for attorney fees, costs, and penalties in an action for a violation of s. 501.1735 or part V of chapter 501 must be deposited in the fund.

Section 27. Except as otherwise expressly provided in this act and except for this section, which shall take effect upon this act becoming a law, this act shall take effect July 1, 2024.

Montana Consumer Data Privacy Act

Section 1. Short title.

[Sections 1 through 12] may be cited as the "Consumer Data Privacy Act".

Section 2. Definitions.

As used in [sections 1 through 12], unless the context clearly indicates otherwise, the following definitions apply:

(1) "Affiliate" means a legal entity that shares common branding with another legal entity or controls, is controlled by, or is under common control with another legal entity.

(2) "Authenticate" means to use reasonable methods to determine that a request to exercise any of the rights afforded under [section 5(1)(a) through (1)(e)] is being made by, or on behalf of, the consumer who is entitled to exercise these consumer rights with respect to the personal data at issue.

(3) (a) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual.

(b) The term does not include:

(i) a digital or physical photograph;

(ii) an audio or video recording; or

(iii) any data generated from a digital or physical photograph or an audio or video recording, unless that data is generated to identify a specific individual.

(4) "Child" means an individual under 13 years of age.

(5) (a) "Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to allow the processing of personal data relating to the consumer. The term may include a written statement, a statement by electronic means, or any other unambiguous affirmative action.

(b) The term does not include:

(i) acceptance of a general or broad term of use or similar document that contains descriptions of personal data processing along with other unrelated information;

(ii) hovering over, muting, pausing, or closing a given piece of content; or

(iii) an agreement obtained using dark patterns.

(6) (a) "Consumer" means an individual who is a resident of this state.

(b) The term does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit, or government agency.

(7) “Control” or “controlled” means:

(a) ownership of or the power to vote more than 50% of the outstanding shares of any class of voting security of a company;

(b) control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or

(c) the power to exercise controlling influence over the management of a company.

(8) “Controller” means an individual who or legal entity that, alone or jointly with others, determines the purpose and means of processing personal data.

(9) “Dark pattern” means a user interface designed or manipulated with the effect of substantially subverting or impairing user autonomy, decision-making, or choice.

(10) “Decisions that produce legal or similarly significant effects concerning the consumer” means decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to necessities such as food and water.

(11) “Deidentified data” means data that cannot be used to reasonably infer information about or otherwise be linked to an identified or identifiable individual or a device linked to the individual if the controller that possesses the data:

(a) takes reasonable measures to ensure that the data cannot be associated with an individual;

(b) publicly commits to process the data in a deidentified fashion only and to not attempt to reidentify the data; and

(c) contractually obligates any recipients of the data to satisfy the criteria set forth in subsections (11)(a) and (11)(b).

(12) “Identified or identifiable individual” means an individual who can be readily identified, directly or indirectly.

(13)“Institution of higher education” means any individual who or school, board, association, limited liability company, or corporation that is licensed or accredited to offer one or more programs of higher learning leading to one or more degrees.

(14) “Nonprofit organization” means any organization that is exempt from taxation under section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the Internal Revenue Code of 1986 or any subsequent corresponding internal revenue code of the United States as amended from time to time.

(15) (a) “Personal data” means any information that is linked or reasonably linkable to an identified or identifiable individual.

(b) The term does not include deidentified data or publicly available information.

(16) (a) “Precise geolocation data” means information derived from technology, including but not limited to global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet.

(b) The term does not include the content of communications, or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(17) “Process” or “processing” means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(18) “Processor” means an individual who or legal entity that processes personal data on behalf of a controller.

(19) "Profiling" means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(20) "Protected health information" has the same meaning as provided in the privacy regulations of the federal Health Insurance Portability and Accountability Act of 1996.

(21) "Pseudonymous data" means personal data that cannot be attributed to a specific individual without the use of additional information, provided the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

(22) "Publicly available information" means information that:

(a) is lawfully made available through federal, state, or municipal government records or widely distributed media; or

(b) a controller has a reasonable basis to believe a consumer has lawfully made available to the public.

(23) (a) "Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party.

(b) The term does not include:

(i) the disclosure of personal data to a processor that processes the personal data on behalf of the controller;

(ii) the disclosure of personal data to a third party for the purposes of providing a product or service requested by the consumer;

(iii) the disclosure or transfer of personal data to an affiliate of the controller;

(iv) the disclosure of personal data in which the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party;

(v) the disclosure of personal data that the consumer:

(A) intentionally made available to the public via a channel of mass media; and

(B) did not restrict to a specific audience; or

(vi) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction, or a proposed merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

(24) "Sensitive data" means personal data that includes:

(a) data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, information about a person's sex life, sexual orientation, or citizenship or immigration status;

(b) the processing of genetic or biometric data for the purpose of uniquely identifying an individual;

(c) personal data collected from a known child; or

(d) precise geolocation data.

(25) (a) "Targeted advertising" means displaying advertisements to a consumer in which the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated internet websites or online applications to predict the consumer's preferences or interests.

(b) The term does not include:

(i) advertisements based on activities within a controller's own internet websites or online applications;

(ii) advertisements based on the context of a consumer's current search query or visit to an internet website or online application;

(iii) advertisements directed to a consumer in response to the consumer's request for information or feedback; or

(iv) processing personal data solely to measure or report advertising frequency, performance, or reach.

(26) "Third party" means an individual or legal entity, such as a public authority, agency, or body, other than the consumer, controller, or processor or an affiliate of the controller or processor.

(27) "Trade secret" has the same meaning as provided in 30-14-402.

Section 3. Applicability.

The provisions of [sections 1 through 12] apply to persons that conduct business in this state or persons that produce products or services that are targeted to residents of this state and:

(1) control or process the personal data of not less than 50,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or

(2) control or process the personal data of not less than 25,000 consumers and derive more than 25% of gross revenue from the sale of personal data.

Section 4. Exemptions.

(1) [Sections 1 through 12] do not apply to any:

(a) body, authority, board, bureau, commission, district, or agency of this state or any political subdivision of this state;

(b) nonprofit organization;

(c) institution of higher education;

(d) national securities association that is registered under 15 U.S.C. 78o-3 of the federal Securities Exchange Act of 1934, as amended;

(e) financial institution or an affiliate of a financial institution governed by, or personal data collected, processed, sold, or disclosed in accordance with, Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801, et seq.; or

(f) covered entity or business associate as defined in the privacy regulations of the federal Health Insurance Portability and Accountability Act of 1996, 45 CFR 160.103.

(2) Information and data exempt from [sections 1 through 12] include:

(a) protected health information under the privacy regulations of the federal Health Insurance Portability and Accountability Act of 1996;

(b) patient-identifying information for the purposes of 42 U.S.C. 290dd-2;

(c) identifiable private information for the purposes of the federal policy for the protection of human subjects of 1991, 45 CFR, part 46;

(d) identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the international council for harmonisation of technical requirements for pharmaceuticals for human use;

(e) the protection of human subjects under 21 CFR, parts 6, 50, and 56, or personal data used or shared in research as defined in the federal Health Insurance Portability and Accountability Act of 1996, 45 CFR 164.501, that is conducted in accordance with the standards set forth in this subsection (2)(e), or other research conducted in accordance with applicable law;

(f) information and documents created for the purposes of the Health Care Quality Improvement Act of 1986, 42 U.S.C. 11101, et seq.;

(g) patient safety work products for the purposes of the Patient Safety and Quality Improvement Act of 2005, 42 U.S.C. 299b-21, et seq., as amended;

(h) information derived from any of the health care-related information listed in this subsection (2) that is:

(i) deidentified in accordance with the requirements for deidentification pursuant to the privacy regulations of the federal Health Insurance Portability and Accountability Act of 1996; or

(ii) included in a limited data set as described in 45 CFR 164.514(e), to the extent that the information is used, disclosed, and maintained in a manner specified in 45 CFR 164.514(e).

(i) information originating from and intermingled to be indistinguishable with or information treated in the same manner as information exempt under this subsection (2) that is maintained by a covered entity or business associate as defined in the privacy regulations of the federal Health Insurance Portability and Accountability Act of 1996, 45 CFR 160.103, or a program or qualified service organization, as specified in 42 U.S.C. 290dd-2, as amended;

(j) information used for public health activities and purposes as authorized by the federal Health Insurance Portability and Accountability Act of 1996, community health activities, and population health activities;

(k) the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, furnisher, or user that provides information for use in a consumer report and by a user of a consumer report, but only to the extent that the activity is regulated by and authorized under the Fair Credit Reporting Act, 15 U.S.C. 1681, as amended;

(l) personal data collected, processed, sold, or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721, et seq., as amended;

(m) personal data regulated by the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. 1232g, et seq., as amended;

(n) personal data collected, processed, sold, or disclosed in compliance with the Farm Credit Act of 1993, 12 U.S.C. 2001, et seq., as amended;

(o) data processed or maintained:

(i) by an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party to the extent that the data is collected and used within the context of that role;

(ii) as the emergency contact information of an individual under [sections 1 through 12] and used for emergency contact purposes; or

(iii) that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under subsection (2)(a) and is used for the purposes of administering the benefits; and

(p) personal data collected, processed, sold, or disclosed in relation to price, route, or service, as these terms are used in the Airline Deregulation Act of 1978, 49 U.S.C. 40101, et seq., as amended, by an air carrier subject to the Airline Deregulation Act of 1978, to the extent [sections 1 through 12] are preempted by the Airline Deregulation Act of 1978, 49 U.S.C. 41713, as amended.

(3) Controllers and processors that comply with the verifiable parental consent requirements of the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501, et seq., shall be considered compliant with any obligation to obtain parental consent pursuant to [sections 1 through 12].

Section 5. Consumer personal data -- opt-out -- compliance -- appeals.

(1) A consumer must have the right to:

(a) confirm whether a controller is processing the consumer's personal data and access the consumer's personal data, unless such confirmation or access would require the controller to reveal a trade secret;

(b) correct inaccuracies in the consumer's personal data, considering the nature of the personal data and the purposes of the processing of the consumer's personal data;

(c) delete personal data about the consumer;

(d) obtain a copy of the consumer's personal data previously provided by the consumer to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the personal data to another controller without hindrance when the processing is carried out by automated means, provided the controller is not required to reveal any trade secret; and

(e) opt out of the processing of the consumer's personal data for the purposes of:

(i) targeted advertising;

(ii) the sale of the consumer's personal data, except as provided in [section 7(2)]; or

(iii) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

(2) A consumer may exercise rights under this section by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice.

(3) (a) A consumer may designate an authorized agent in accordance with [section 6] to exercise the rights of the consumer to opt out of the processing of the consumer's personal data under subsection (1)(e) on behalf of the consumer.

(b) A parent or legal guardian of a known child may exercise the consumer rights on the known child's behalf regarding the processing of personal data.

(c) A guardian or conservator of a consumer subject to a guardianship, conservatorship, or other protective arrangement, may exercise the rights on the consumer's behalf regarding the processing of personal data.

(4) Except as otherwise provided in [sections 1 through 12], a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to this section as follows:

(a) A controller shall respond to the consumer without undue delay, but not later than 45 days after receipt of the request. The controller may extend the response period by 45 additional days when reasonably necessary, considering the complexity and number of the consumer's requests, provided the controller informs the consumer of the extension within the initial 45-day response period and the reason for the extension.

(b) If a controller declines to act regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than 45 days after receipt of the request, of the justification for declining to act and provide instructions for how to appeal the decision.

(c) Information provided in response to a consumer request must be provided by a controller, free of charge, once for each consumer during any 12-month period. If requests from a consumer are manifestly unfounded, excessive, technically infeasible, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive, technically infeasible, or repetitive nature of the request.

(d) If a controller is unable to authenticate a request to exercise any of the rights afforded under subsections (1)(a) through (1)(d) of this section using commercially reasonable efforts, the controller may not be required to comply with a request to initiate an action pursuant to this section and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise the right or rights until the consumer provides additional information reasonably necessary to authenticate the consumer and the consumer's request to exercise the consumer's rights. A controller may not be required to authenticate an opt-out request, but a controller may deny an opt-out request if the controller has a good faith, reasonable, and documented belief that the request is fraudulent. If a controller denies an opt-out request because the controller believes the request is fraudulent, the controller shall send notice to the person who made the request disclosing that the controller believes the request is fraudulent and that the controller may not comply with the request.

(e) A controller that has obtained personal data about a consumer from a source other than the consumer must be deemed in compliance with the consumer's request to delete the consumer's data pursuant to subsection (1)(c) by:

(i) retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the controller's records and not using the retained data for any other purpose pursuant to the provisions of [sections 1 through 12]; or

(ii) opting the consumer out of the processing of the consumer's personal data for any purpose except for those exempted pursuant to the provisions of [sections 1 through 12].

(5) A controller shall establish a process for a consumer to appeal the controller's refusal to act on a request within a reasonable period after the consumer's receipt of the decision. The appeal process must be conspicuously available and like the process for submitting requests to initiate action pursuant to this section. Not later than 60 days after receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a

written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general to submit a complaint.

Section 6. Authorized agent.

(1) A consumer may designate another person to serve as the consumer's authorized agent and act on the consumer's behalf to opt out of the processing of the consumer's personal data for one or more of the purposes specified in [section 5(1)(e)]. The consumer may designate an authorized agent by way of a technology, including but not limited to an internet link or a browser setting, browser extension, or global device setting indicating a customer's intent to opt out of such processing.

(2) A controller shall comply with an opt-out request received from an authorized agent if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf.

(3) Opt-out methods must:

(a) provide a clear and conspicuous link on the controller's internet website to an internet web page that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising or sale of the consumer's personal data; and

(b) by no later than January 1, 2025, allow a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data through an opt-out preference signal sent with the consumer's consent, to the controller by a platform, technology, or mechanism that:

(i) may not unfairly disadvantage another controller; (ii) may not make use of a default setting, but require the consumer to make an affirmative, freely given and unambiguous choice to opt out of any processing of a customer's personal data pursuant to [sections 1 through 12];

(iii) must be consumer-friendly and easy to use by the average consumer;

(iv) must be consistent with any federal or state law or regulation; and

(v) must allow the controller to accurately determine whether the consumer is a resident of the state and whether the consumer has made a legitimate request to opt out of any sale of a consumer's personal data or targeted advertising.

(4) (a) If a consumer's decision to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of personal data, through an opt-out preference signal sent in accordance with the provisions of subsection (3) conflicts with the consumer's existing controller-specific privacy setting or voluntary participation in a controller's bona fide loyalty, rewards, premium features, discounts, or club card program, the controller shall comply with the consumer's opt-out preference signal but may notify the consumer of the conflict and provide the choice to confirm controller-specific privacy settings or participation in such a program.

(b) If a controller responds to consumer opt-out requests received in accordance with subsection (3) by informing the consumer of a charge for the use of any product or service, the controller shall present the terms of any financial incentive offered pursuant to subsection (3) for the retention, use, sale, or sharing of the consumer's personal data.

Section 7. Data processing by controller -- limitations.

(1) A controller shall:

(a) limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the personal data is processed, as disclosed to the consumer;

(b) establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue; and

(c) provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, on revocation of the consent, cease to process the personal data as soon as practicable, but not later than 45 days after the receipt of the request.

(2) A controller may not:

(a) except as otherwise provided in [sections 1 through 12], process personal data for purposes that are not reasonably necessary to or compatible with the disclosed purposes for which the personal data is processed as disclosed to the consumer unless the controller obtains the consumer's consent;

(b) process sensitive data concerning a consumer without obtaining the consumer's consent or, in the case of the processing of sensitive data concerning a known child, without processing the sensitive data in accordance with the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501, et seq.;

(c) process personal data in violation of the laws of this state and federal laws that prohibit unlawful discrimination against consumers;

(d) process the personal data of a consumer for the purposes of targeted advertising or sell the consumer's personal data without the consumer's consent under circumstances in which a controller has actual knowledge that the consumer is at least 13 years of age but younger than 16 years of age; or

(e) discriminate against a consumer for exercising any of the consumer rights contained in [sections 1 through 12], including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer.

(3) Nothing in subsection (1) or (2) may be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised their right to opt out pursuant to [sections 1 through 12] or the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

(4) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose the processing, as well as the way a consumer may exercise the right to opt out of the processing.

(5) A controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

(a) the categories of personal data processed by the controller;

(b) the purpose for processing personal data;

(c) the categories of personal data that the controller shares with third parties, if any;

(d) the categories of third parties, if any, with which the controller shares personal data; and

(e) an active e-mail address or other mechanism that the consumer may use to contact the controller; and

(f) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision regarding the consumer's request.

(6) (a) A controller shall establish and describe in a privacy notice one or more secure and reliable means for consumers to submit a request to exercise their consumer rights pursuant to [sections 1 through 12] considering the ways in which consumers normally interact with the controller, the need for secure and reliable communication of consumer requests, and the ability of the controller to verify the identity of the consumer making the request.

(b) A controller may not require a consumer to create a new account to exercise consumer rights but may require a consumer to use an existing account.

Section 8. Data processor -- allowances -- limitations.

(1) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under [sections 1 through 12] to include:

(a) considering the nature of processing and the information available to the processor by appropriate technical and organizational measures as much as reasonably practicable to fulfill the controller's obligation to respond to consumer rights requests;

(b) considering the nature of processing and the information available to the processor by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security, as provided for in 30-14-1704, of the system of the processor to meet the controller's obligations; and

(c) providing necessary information to enable the controller to conduct and document data protection assessments.

(2) A contract between a controller and a processor must govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract must be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract must also require that the processor:

(a) ensure that each person processing personal data is subject to a duty of confidentiality with respect to the personal data;

(b) at the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

(c) on the reasonable request of the controller, make available to the controller all information in the processor's possession necessary to demonstrate the processor's compliance with the obligations in [sections 1 through 12];

(d) engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data; and

(e) allow and cooperate with reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to assess the processor's policies and technical and organizational measures in support of the obligations under [sections 1 through 12] using an appropriate and accepted control standard or framework and assessment procedure for the assessments. The processor shall provide a report of the assessment to the controller on request.

(3) Nothing in this section may be construed to relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of the controller's or processor's role in the processing relationship, as described in [sections 1 through 12].

(4) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends on the following context in which personal data is to be processed:

(a) A person who is not limited in the processing of personal data pursuant to a controller's instructions or who fails to adhere to a controller's instructions is a controller and not a processor with respect to a specific processing of data.

(b) A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor.

(c) If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to the processing and may be subject to an enforcement action under [section 12].

Section 9. Data protection assessment.

(1) A controller shall conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer. For the purposes of this section, processing that presents a heightened risk of harm to a consumer includes:

(a) the processing of personal data for the purposes of targeted advertising;

(b) the sale of personal data;

(c) the processing of personal data for the purposes of profiling in which the profiling presents a reasonably foreseeable risk of:

(i) unfair or deceptive treatment of or unlawful disparate impact on consumers;

(ii) financial, physical, or reputational injury to consumers;

(iii) a physical or other form of intrusion on the solitude or seclusion or the private affairs or concerns of consumers in which the intrusion would be offensive to a reasonable person; or

(iv) other substantial injury to consumers; and

(d) the processing of sensitive data.

(2) (a) Data protection assessments conducted pursuant to subsection (1) must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing as mitigated by safeguards that may be employed by the controller to reduce these risks.

(b) The controller shall factor into any data protection assessment the use of deidentified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

(3) (a) The attorney general may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the attorney general, and the controller shall make the data protection assessment available to the attorney general.

(b) The attorney general may evaluate the data protection assessment for compliance with the responsibilities set forth in [sections 1 through 12].

(c) Data protection assessments are confidential and are exempt from disclosure under the Freedom of Information Act, 5 U.S.C. 552.

(d) To the extent any information contained in a data protection assessment disclosed to the attorney general includes information subject to attorney-client privilege or work product protection, the disclosure may not constitute a waiver of the privilege or protection.

(4) A single data protection assessment may address a comparable set of processing operations that include similar activities.

(5) If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment must be considered to satisfy the requirements established in this section if the data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.

(6) Data protection assessment requirements must apply to processing activities created or generated after January 1, 2025, and are not retroactive.

Section 10. Deidentified data.

(1) Any controller in possession of deidentified data shall:

(a) take reasonable measures to ensure that the deidentified data cannot be associated with an individual;

(b) publicly commit to maintaining and using deidentified data without attempting to reidentify the deidentified data; and

(c) contractually obligate any recipients of the deidentified data to comply with all provisions of [sections 1 through 12].

(2) Nothing in [sections 1 through 12] may be construed to:

(a) require a controller or processor to reidentify deidentified data or pseudonymous data; or

(b) maintain data in identifiable form or collect, obtain, retain, or access any data or technology to be capable of associating an authenticated consumer request with personal data.

(3) Nothing in [sections 1 through 12] may be construed to require a controller or processor to comply with an authenticated consumer rights request if the controller:

(a) is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data;

(b) does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data or associate the personal data with other personal data about the same specific consumer; and

(c) does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.

(4) The rights afforded under [section 5(1)(a) through (1)(d)] may not apply to pseudonymous data in cases in which the controller is able to demonstrate that any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

(5) A controller that discloses pseudonymous data or deidentified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or deidentified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

Section 11. Compliance by controller or processor.

(1) Nothing in [sections 1 through 12] may be construed to restrict a controller's or processor's ability to:

(a) comply with federal, state, or municipal ordinances or regulations;

(b) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, municipal, or other government authorities;

(c) cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or municipal ordinances or regulations;

(d) investigate, establish, exercise, prepare for, or defend legal claims;

(e) provide a product or service specifically requested by a consumer;

(f) perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty;

(g) take steps at the request of a consumer prior to entering a contract;

(h) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual and when the processing cannot be manifestly based on another legal basis;

(i) prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity, preserve the integrity or security of systems, or investigate, report, or prosecute those responsible for any of these actions;

(j) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board that determines or similar independent oversight entities that determine:

(A) whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller;

(B) the expected benefits of the research outweigh the privacy risks; and

(C) whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification;

(k) assist another controller, processor, or third party with any of the obligations under [sections 1 through 12]; or

(I) process personal data for reasons of public interest in public health, community health, or population health, but solely to the extent that the processing is:

(A) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed; and

(B) under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law.

(2) The obligations imposed on controllers or processors under [sections 1 through 12] may not restrict a controller's or processor's ability to collect, use, or retain personal data for internal use to:

(a) conduct internal research to develop, improve, or repair products, services, or technology;

(b) effectuate a product recall;

(c) identify and repair technical errors that impair existing or intended functionality; or

(d) perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

(3) The obligations imposed on controllers or processors under [sections 1 through 12] may not apply when compliance by the controller or processor with [sections 1 through 12] would violate an evidentiary privilege under the laws of this state. Nothing in [sections 1 through 12] may be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of this state as part of a privileged communication.

(4) A controller or processor that discloses personal data to a processor or third-party controller in accordance with [sections 1 through 12] may not be considered to have violated [sections 1 through 12] if the processor or third-party controller that receives and processes the personal data violates [sections 1 through 12] provided, at the time the disclosing controller or processor disclosed the personal data, the disclosing controller or processor did not have actual knowledge that the receiving processor or third-party controller would violate [sections 1 through 12]. A receiving processor or third-party controller receiving personal data from a disclosing controller or processor in compliance with [sections 1 through 12] is likewise not in violation of [sections 1 through 12] for the transgressions of the disclosing controller or processor from which the receiving processor or third-party controller receives the personal data.

(5) Nothing in [sections 1 through 12] may be construed to:

(a) impose any obligation on a controller or processor that adversely affects the rights or freedoms of any person, including but not limited to the rights of any person:

(i) to freedom of speech or freedom of the press guaranteed in the first amendment to the United States constitution; or

(ii) under Rule 504 of the Montana Rules of Evidence; or

(b) apply to a person's processing of personal data during the person's personal or household activities.

(6) Personal data processed by a controller pursuant to this section may be processed to the extent that the processing is:

(a) reasonably necessary and proportionate to the purposes listed in this section; and

(b) adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section. The controller or processor must, when applicable, consider the nature and purpose of the collection, use, or retention of the personal data collected, used, or retained pursuant to subsection (2). The personal data must be subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to the collection, use, or retention of personal data.

(7) If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that the processing qualifies for the exemption and complies with the requirements in subsection (6).

(8) Processing personal data for the purposes expressly identified in this section may not solely make a legal entity a controller with respect to the processing.

Section 12. Enforcement.

(1) The attorney general has exclusive authority to enforce violations pursuant to [sections 1 through 11].

(2) (a) The attorney general shall, prior to initiating any action for a violation of any provision of [sections 1 through 11], issue a notice of violation to the controller.

(b) If the controller fails to correct the violation within 60 days of receipt of the notice of violation, the attorney general may bring an action pursuant to this section.

(c) If within the 60-day period the controller corrects the noticed violation and provides the attorney general an express written statement that the alleged violations have been corrected and that no such further violations will occur, no action must be initiated against the controller.

(3) Nothing in [sections 1 through 11] may be construed as providing the basis for or be subject to a private right of action for violations of [sections 1 through 11] or any other law.

Section 13. Codification instruction.

[Sections 1 through 12] are intended to be codified as an integral part of Title 30, chapter 14, and the provisions of Title 30, chapter 14, apply to [sections 1 through 12].

Section 14. Effective date.

[This act] is effective October 1, 2024.

Section 15. Termination.

[Section 12(2)] terminates April 1, 2026.

Oregon Privacy Act

SECTION 1.

As used in sections 1 to 9 of this 2023 Act:

(1) "Affiliate" means a person that, directly or indirectly through one or more intermediaries, controls, is controlled by or is under common control with another person such that:

(a) The person owns or has the power to vote more than 50 percent of the outstanding shares of any voting class of the other person's securities;

(b) The person has the power to elect or influence the election of a majority of the directors, members or managers of the other person;

(c) The person has the power to direct the management of another person; or

(d) The person is subject to another person's exercise of the powers described in paragraph (a), (b) or (c) of this subsection.

(2) "Authenticate" means to determine, using commercially reasonable methods, whether a consumer with the rights described in section 3 of this 2023 Act, or a person acting on behalf of the consumer, is the consumer who has asked to exercise, or is a person who has authority to exercise, any of the consumer's rights.

(3)(a) "Biometric data" means personal data generated by automatic measurements of a consumer's biological characteristics, such as the consumer's fingerprint, voiceprint, retinal pattern, iris pattern, gait or other unique biological characteristics that allow or confirm the unique identification of the consumer.

(b) "Biometric data" does not include:

(A) A photograph recorded digitally or otherwise;

(B) An audio or video recording;

(C) Data from a photograph or from an audio or video recording, unless the data were generated for the purpose of identifying a specific consumer or were used to identify a particular consumer; or

(D) Facial mapping or facial geometry, unless the facial mapping or facial geometry was generated for the purpose of identifying a specific consumer or was used to identify a specific consumer.

(4) "Business associate" has the meaning given that term in 45 C.F.R. 160.103, as in effect on the effective date of this 2023 Act.

(5) "Child" means an individual under the age of 13.

(6) "Consent" means an affirmative act by means of which a consumer clearly and conspicuously communicates the consumer's freely given, specific, informed and unambiguous assent to another person's act or practice under the following conditions:

(a) The user interface by means of which the consumer performs the act does not have any mechanism that has the purpose or substantial effect of obtaining consent by obscuring, subverting or impairing the consumer's autonomy, decision-making or choice; and

(b) The consumer's inaction does not constitute consent.

(7) "Consumer" means a natural person who resides in this state and acts in any capacity other than in a commercial or employment context.

(8) “Controller” means a person that, alone or jointly with another person, determines the purposes and means for processing personal data.

(9) “Covered entity” has the meaning given that term in 45 C.F.R. 160.103, as in effect on the effective date of this 2023 Act.

(10) “Decisions that produce legal effects or effects of similar significance” means decisions that result in providing or denying financial or lending services, housing, insurance, enrollment in education or educational opportunity, criminal justice, employment opportunities, health care services or access to essential goods and services.

(11) “Deidentified data” means data that:

(a) Cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable consumer, or to a device that identifies, is linked to or is reasonably linkable to a consumer; or

(b) Is:

(A) Derived from patient information that was originally created, collected, transmitted or maintained by an entity subject to regulation under the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, as in effect on the effective date of this 2023 Act, or the Federal Policy for the Protection of Human Subjects, codified as 45 C.F.R. part 46 and in various other deferral regulations, as codified in various sections of the Code of Federal Regulations and as in effect on the effective date of this 2023 Act; and

(B) Deidentified as provided in 45 C.F.R. 164.514, as in effect on the effective date of this 2023 Act.

(12) “Device” means electronic equipment designed for a consumer’s use that can transmit or receive personal data.

(13)(a) “Personal data” means data, derived data or any unique identifier that is linked to or is reasonably linkable to a consumer or to a device that identifies, is linked to or is reasonably linkable to one or more consumers in a household.

(b) “Personal data” does not include deidentified data or data that:

(A) Is lawfully available through federal, state or local government records or through widely distributed media; or

(B) A controller reasonably has understood to have been lawfully made available to the public by a consumer.

(14) “Process” or “processing” means an action, operation or set of actions or operations that is performed, automatically or otherwise, on personal data or on sets of personal data, such as collecting, using, storing, disclosing, analyzing, deleting or modifying the personal data.

(15) “Processor” means a person that processes personal data on behalf of a controller.

(16) “Profiling” means an automated processing of personal data for the purpose of evaluating, analyzing or predicting an identified or identifiable consumer’s economic circumstances, health, personal preferences, interests, reliability, behavior, location or movements.

(17)(a) “Sale” or “sell” means the exchange of personal data for monetary or other valuable consideration by the controller with a third party.

(b) “Sale” or “sell” does not include:

(A) A disclosure of personal data to a processor;

(B) A disclosure of personal data to an affiliate of a controller or to a third party for the purpose of enabling the controller to provide a product or service to a consumer that requested the product or service;

(C) A disclosure or transfer of personal data from a controller to a third party as part of a proposed or completed merger, acquisition, bankruptcy or other transaction in which the third party assumes control of all or part of the controller's assets, including the personal data; or

(D) A disclosure of personal data that occurs because a consumer:

(i) Directs a controller to disclose the personal data;

(ii) Intentionally discloses the personal data in the course of directing a controller to interact with a third party; or

(iii) Intentionally discloses the personal data to the public by means of mass media, if the disclosure is not restricted to a specific audience.

(18)(a) "Sensitive data" means personal data that:

(A) Reveals a consumer's racial or ethnic background, national origin, religious beliefs, mental or physical condition or diagnosis, sexual orientation, status as transgender or nonbinary, status as a victim of crime or citizenship or immigration status;

(B) Is a child's personal data;

(C) Accurately identifies within a radius of 1,750 feet a consumer's present or past location, or the present or past location of a device that links or is linkable to a consumer by means of technology that includes, but is not limited to, a global positioning system that provides latitude and longitude coordinates; or

(D) Is genetic or biometric data.

(b) "Sensitive data" as defined in paragraph (a)(C) of this subsection does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(19)(a) "Targeted advertising" means advertising that is selected for display to a consumer on the basis of personal data obtained from the consumer's activities over time and across one or more unaffiliated websites or online applications and is used to predict the consumer's preferences or interests.

(b) "Targeted advertising" does not include:

(A) Advertisements that are based on activities within a controller's own websites or online applications;

(B) Advertisements based on the context of a consumer's current search query, visit to a specific website or use of an online application;

(C) Advertisements that are directed to a consumer in response to the consumer's request for information or feedback; or

(D) A processing of personal data solely for the purpose of measuring or reporting an advertisement's frequency, performance or reach.

(20) "Third party" means a person, a public corporation, including the Oregon Health and Science University and the Oregon State Bar, or a public body, as defined in ORS 174.109, other than a consumer, a controller, a processor or an affiliate of a controller or processor.

SECTION 2.

(1) Sections 1 to 9 of this 2023 Act apply to any person that conducts business in this state, or that provides products or services to residents of this state, and that during a calendar year, controls or processes:

(a) The personal data of 100,000 or more consumers, other than personal data controlled or processed solely for the purpose of completing a payment transaction; or

(b) The personal data of 25,000 or more consumers, while deriving 25 percent or more of the person's annual gross revenue from selling personal data.

(2) Sections 1 to 9 of this 2023 Act do not apply to:

(a) A public corporation, including the Oregon Health and Science University and the Oregon State Bar, or a public body, as defined in ORS 174.109;

(b) Protected health information that a covered entity or business associate processes in accordance with, or documents that a covered entity or business associate creates for the purpose of complying with, the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, and regulations promulgated under the Act, as in effect on the effective date of this 2023 Act;

(c) Information used only for public health activities and purposes described in 45 C.F.R. 164.512, as in effect on the effective date of this 2023 Act;

(d) Information that identifies a consumer in connection with:

(A) Activities that are subject to the Federal Policy for the Protection of Human Subjects, codified as 45 C.F.R. part 46 and in various other federal regulations, as in effect on the effective date of this 2023 Act;

(B) Research on human subjects undertaken in accordance with good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use;

(C) Activities that are subject to the protections provided in 21 C.F.R. parts 50 and 56, as in effect on the effective date of this 2023 Act; or

(D) Research conducted in accordance with the requirements set forth in subparagraphs (A) to (C) of this paragraph or otherwise in accordance with applicable law;

(e) Patient identifying information, as defined in 42 C.F.R. 2.11, as in effect on the effective date of this 2023 Act, that is collected and processed in accordance with 42 C.F.R. part 2;

(f) Patient safety work product, as defined in 42 C.F.R. 3.20, as in effect on the effective date of this 2023 Act, that is created for purposes of improving patient safety under 42 C.F.R. part 3;

(g) Information and documents created for the purposes of the Health Care Quality Improvement Act of 1986, 42 U.S.C. 11101 et seq., and implementing regulations, both as in effect on the effective date of this 2023 Act;

(h) Information that originates from, or that is intermingled so as to be indistinguishable from, information described in paragraphs (b) to (g) of this subsection that a covered entity or business associate, or a program of a qualified service organization, as defined in 42 C.F.R. 2.11, as in effect on the effective date of this 2023 Act, creates, collects, processes, uses or maintains in the same manner as is required under the laws, regulations and guidelines described in paragraphs (b) to (g) of this subsection;

(i) Information processed or maintained solely in connection with, and for the purpose of, enabling:

(A) An individual's employment or application for employment;

(B) An individual's ownership of, or function as a director or officer of, a business entity;

(C) An individual's contractual relationship with a business entity;

(D) An individual's receipt of benefits from an employer, including benefits for the individual's dependents or beneficiaries; or

(E) Notice of an emergency to persons that an individual specifies;

(j) Any activity that involves collecting, maintaining, disclosing, selling, communicating or using information for the purpose of evaluating a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living if done strictly in accordance with the provisions of the Fair Credit Reporting Act, 15 U.S.C. 1681 et seq., as in effect on the effective date of this 2023 Act, by:

(A) A consumer reporting agency, as defined in 15 U.S.C. 1681a(f), as in effect on the effective date of this 2023 Act;

(B) A person who furnishes information to a consumer reporting agency under 15 U.S.C. 1681s-2, as in effect on the effective date of this 2023 Act; or

(C) A person who uses a consumer report as provided in 15 U.S.C. 1681b(a)(3);

(k) Information collected, processed, sold or disclosed under and in accordance with the following federal laws, all as in effect on the effective date of this 2023 Act:

(A) The Gramm-Leach-Bliley Act, P.L. 106-102, and regulations adopted to implement that Act;

(B) The Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721 et seq.;

(C) The Family Educational Rights and Privacy Act, 20 U.S.C. 1232g and regulations adopted to implement that Act; and

(D) The Airline Deregulation Act, P.L. 95-504, only to the extent that an air carrier collects information related to prices, routes or services and only to the extent that the provisions of the Airline Deregulation Act preempt sections 1 to 9 of this 2023 Act;

(l) A financial institution, as defined in ORS 706.008, or a financial institution's affiliate or subsidiary that is only and directly engaged in financial activities, as described in 12 U.S.C. 1843(k), as in effect on the effective date of this 2023 Act;

(m) Information that originates from, or is intermingled so as to be indistinguishable from, information described in paragraph (k)(A) of this subsection and that a licensee, as defined in ORS 725.010, collects, processes, uses or maintains in the same manner as is required under the laws and regulations specified in paragraph (k)(A) of this subsection;

(n) An insurer, as defined in ORS 731.106, other than a person that, alone or in combination with another person, establishes and maintains a self-insurance program and that does not otherwise engage in the business of entering into policies of insurance;

(o) An insurance producer, as defined in ORS 731.104;

(p) An insurance consultant, as defined in ORS 744.602;

(q) A person that holds a third party administrator license issued under ORS 744.710;

(r) A nonprofit organization that is established to detect and prevent fraudulent acts in connection with insurance; and

(s) Noncommercial activity of:

(A) A publisher, editor, reporter or other person who is connected with or employed by a newspaper, magazine, periodical, newsletter, pamphlet, report or other publication in general circulation;

(B) A radio or television station that holds a license issued by the Federal Communications Commission;

(C) A nonprofit organization that provides programming to radio or television networks; or

(D) An entity that provides an information service, including a press association or wire service.

(3) Sections 1 to 9 of this 2023 Act do not prohibit a controller or processor from:

(a) Complying with federal, state or local statutes, ordinances, rules or regulations;

(b) Complying with a federal, state or local governmental inquiry, investigation, subpoena or summons related to a civil, criminal or administrative proceeding;

(c) Cooperating with a law enforcement agency concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state or local statutes, ordinances, rules or regulations;

(d) Investigating, establishing, initiating or defending legal claims;

(e) Preventing, detecting, protecting against or responding to, and investigating, reporting or prosecuting persons responsible for, security incidents, identity theft, fraud, harassment or malicious, deceptive or illegal activity or preserving the integrity or security of systems;

(f) Identifying and repairing technical errors in a controller's or processor's information systems that impair existing or intended functionality;

(g) Providing a product or service that a consumer specifically requests from the controller or processor or requests as the parent or guardian of a child on the child's behalf or as the guardian or conservator of a person subject to a guardianship, conservatorship or other protective arrangement on the person's behalf;

(h) Negotiating, entering into or performing a contract with a consumer, including fulfilling the terms of a written warranty;

(i) Protecting any person's health and safety;

(j) Effectuating a product recall;

(k) Conducting internal research to develop, improve or repair products, services or technology;

(l) Performing internal operations that are reasonably aligned with a consumer's expectations, that the consumer may reasonably anticipate based on the consumer's existing relationship with the controller or that are otherwise compatible with processing data for the purpose of providing a product or service the consumer specifically requested or for the purpose of performing a contract to which the consumer is a party; or

(m) Assisting another controller or processor with any of the activities set forth in this subsection.

(4) Sections 1 to 9 of this 2023 Act do not apply to the extent that a controller's or processor's compliance with sections 1 to 9 of this 2023 Act would violate an evidentiary privilege under the laws of this state. Notwithstanding the provisions of sections 1 to 9 of this 2023 Act, a controller or processor may provide personal data about a consumer in a privileged communication to a person that is covered by an evidentiary privilege under the laws of this state.

(5) A controller may process personal data in accordance with subsection (3) of this section only to the extent that the processing is adequate and reasonably necessary for, relevant to, proportionate in relation to and limited to the purposes set forth in this section.

(6) Collection, use and retention of personal data under subsection (3)(e) and (f) of this section must, where applicable, take into account the nature and purpose of the collection, use or retention. The personal data must be subject to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and security of the personal data and reduce reasonably foreseeable risks of harm to consumers from the collection, use or retention.

(7) A controller that claims that the controller's processing of personal data is exempt under subsection (3) of this section has the burden of demonstrating that the controller's processing qualifies for the exemption and complies with the requirements of subsections (5) and (6) of this section.

SECTION 3.

(1) Subject to section 4 of this 2023 Act, a consumer may:

(a) Obtain from a controller:

(A) Confirmation as to whether the controller is processing or has processed the consumer's personal data and the categories of personal data the controller is processing or has processed;

(B) At the controller's option, a list of specific third parties, other than natural persons, to which the controller has disclosed:

(i) The consumer's personal data; or

(ii) Any personal data; and

(C) A copy of all of the consumer's personal data that the controller has processed or is processing;

(b) Require a controller to correct inaccuracies in personal data about the consumer, taking into account the nature of the personal data and the controller's purpose for processing the personal data;

(c) Require a controller to delete personal data about the consumer, including personal data the consumer provided to the controller, personal data the controller obtained from another source and derived data; or

(d) Opt out from a controller's processing of personal data of the consumer that the controller processes for any of the following purposes:

(A) Targeted advertising;

(B) Selling the personal data; or

(C) Profiling the consumer in furtherance of decisions that produce legal effects or effects of similar significance.

(2) A controller that provides a copy of personal data to a consumer under subsection (1)(a)(C) of this section shall provide the personal data in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the personal data to another person without hindrance.

(3) This section does not require a controller to disclose the controller's trade secrets, as defined in ORS 646.461.

SECTION 4.

(1) A consumer may exercise the rights described in section 3 of this 2023 Act by submitting a request to a controller using the method that the controller specifies in the privacy notice described in section 5 of this 2023 Act.

(2) A controller may not require a consumer to create an account for the purpose described in subsection (1) of this section, but the controller may require the consumer to use an account the consumer created previously.

(3) A parent or legal guardian may exercise the rights described in section 3 of this 2023 Act on behalf of the parent's child or on behalf of a child for whom the guardian has legal responsibility. A guardian or conservator may exercise the rights described in subsection (1) of this section on behalf of a consumer that is subject to a guardianship, conservatorship or other protective arrangement.

(4) A consumer may designate another person to act on the consumer's behalf as the consumer's authorized agent for the purpose of opting out of a controller's processing of the consumer's personal data, as provided in section 3 (1)(d) of this 2023 Act. The consumer may designate an authorized agent by means of an internet link, browser setting, browser extension, global device setting or other technology that enables the consumer to opt out of the controller's processing of the consumer's personal data. A controller shall comply with an opt-out request the controller receives from an authorized agent if the controller can verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf.

(5) Except as otherwise provided in sections 1 to 9 of this 2023 Act, in responding to a request under subsection (1) of this section, a controller shall:

(a) Respond to a request from a consumer without undue delay and not later than 45 days after receiving the request. The controller may extend the period within which the controller responds by an additional 45 days if the extension is reasonably necessary to comply with the consumer's request, taking into consideration the complexity of the request and the number of requests the consumer makes. A controller that intends to extend the period for responding shall notify the consumer within the initial 45-day response period and explain the reason for the extension.

(b) Notify the consumer without undue delay and not later than 45 days after receiving the consumer's request if the controller declines to take action on the request. The controller in the notice shall explain the justification for not taking action and include instructions for appealing the controller's decision.

(c) Provide information the consumer requests once during any 12-month period without charge to the consumer. A controller may charge a reasonable fee to cover the administrative costs of complying with a second or subsequent request within the 12-month period, unless the purpose of the second or subsequent request is to verify that the controller corrected inaccuracies in, or deleted, the consumer's personal data in compliance with the consumer's request.

(d) Notify the consumer if the controller cannot, using commercially reasonable methods, authenticate the consumer's request without additional information from the consumer. A controller that sends a notification under this paragraph does not have to comply with the request until the consumer provides the information necessary to authenticate the request.

(e) Comply with a request under section 3 (1)(d) of this 2023 Act to opt out of the controller's processing of the consumer's personal data without requiring authentication, except that:

(A) A controller may ask for additional information necessary to comply with the request, such as information that is necessary to identify the consumer that requested to opt out.

(B) A controller may deny a request to opt out if the controller has a good-faith, reasonable and documented belief that the request is fraudulent. If the controller denies a request under this subparagraph, the controller shall notify the consumer that the controller believes the request is fraudulent, stating in the notice that the controller will not comply with the request.

(6) A controller shall establish a process by means of which a consumer may appeal the controller's refusal to take action on a request under subsection (1) of this section. The controller's process must:

(a) Allow a reasonable period of time after the consumer receives the controller's refusal within which to appeal;

(b) Be conspicuously available to the consumer;

(c) Be similar to the manner in which a consumer must submit a request under subsection (1) of this section; and

(d) Require the controller to approve or deny the appeal within 45 days after the date on which the controller received the appeal and to notify the consumer in writing of the controller's decision and the reasons for the decision. If the controller denies the appeal, the notice must provide or specify information that enables the consumer to contact the Attorney General to submit a complaint.

(7) A controller that obtains personal data about a consumer from a source other than the consumer complies with the consumer's request to delete the personal data if the controller:

(a) Deletes the data but retains a record of the deletion request and a minimal amount of data necessary to ensure that the personal data remains deleted and does not use the minimal data for any other purpose; or

(b) Opts the consumer out of the controller's processing of the consumer's personal data for any purpose other than a purpose that is exempt under section 2 of this 2023 Act.

SECTION 5.

(1) A controller shall:

(a) Specify in the privacy notice described in subsection (4) of this section the express purposes for which the controller is collecting and processing personal data;

(b) Limit the controller's collection of personal data to only the personal data that is adequate, relevant and reasonably necessary to serve the purposes the controller specified in paragraph (a) of this subsection;

(c) Establish, implement and maintain for personal data the same safeguards described in ORS 646A.622 that are required for protecting personal information, as defined in ORS 646A.602, such that the controller's safeguards protect the confidentiality, integrity and accessibility of the personal data to the extent appropriate for the volume and nature of the personal data; and

(d) Provide an effective means by which a consumer may revoke consent a consumer gave under sections 1 to 9 of this 2023 Act to the controller's processing of the consumer's personal data. The means must be at least as easy as the means by which the consumer provided consent. Once the consumer revokes consent, the controller shall cease processing the personal data as soon as is practicable, but not later than 15 days after receiving the revocation.

(2) A controller may not:

(a) Process personal data for purposes that are not reasonably necessary for and compatible with the purposes the controller specified in subsection (1)(a) of this section, unless the controller obtains the consumer's consent;

(b) Process sensitive data about a consumer without first obtaining the consumer's consent or, if the controller knows the consumer is a child, without processing the sensitive data in accordance with the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501 et seq. and the regulations, rules and guidance adopted under the Act, all as in effect on the effective date of this 2023 Act;

(c) Process a consumer's personal data for the purposes of targeted advertising, of profiling the consumer in furtherance of decisions that produce legal effects or effects of similar significance or of selling the consumer's personal data without the consumer's consent if the controller has actual knowledge that, or willfully disregards whether, the consumer is at least 13 years of age and not older than 15 years of age; or

(d) Discriminate against a consumer that exercises a right provided to the consumer under sections 1 to 9 of this 2023 Act by means such as denying goods or services, charging different prices or rates for goods or services or providing a different level of quality or selection of goods or services to the consumer.

(3) Subsections (1) and (2) of this section do not:

(a) Require a controller to provide a good or service that requires personal data from a consumer that the controller does not collect or maintain; or

(b) Prohibit a controller from offering a different price, rate, level of quality or selection of goods or services to a consumer, including an offer for no fee or charge, in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discount or club card program.

(4) A controller shall provide to consumers a reasonably accessible, clear and meaningful privacy notice that:

(a) Lists the categories of personal data, including the categories of sensitive data, that the controller processes;

(b) Describes the controller's purposes for processing the personal data;

(c) Describes how a consumer may exercise the consumer's rights under sections 1 to 9 of this 2023 Act, including how a consumer may appeal a controller's denial of a consumer's request under section 4 of this 2023 Act;

(d) Lists all categories of personal data, including the categories of sensitive data, that the controller shares with third parties;

(e) Describes all categories of third parties with which the controller shares personal data at a level of detail that enables the consumer to understand what type of entity each third party is and, to the extent possible, how each third party may process personal data;

(f) Specifies an electronic mail address or other online method by which a consumer can contact the controller that the controller actively monitors;

(g) Identifies the controller, including any business name under which the controller registered with the Secretary of State and any assumed business name that the controller uses in this state;

(h) Provides a clear and conspicuous description of any processing of personal data in which the controller engages for the purpose of targeted advertising or for the purpose of profiling the consumer in furtherance of decisions that produce legal effects or effects of similar significance, and a procedure by which the consumer may opt out of this type of processing; and

(i) Describes the method or methods the controller has established for a consumer to submit a request under section 4 (1) of this 2023 Act.

(5) The method or methods described in subsection (4)(i) of this section for submitting a consumer's request to a controller must:

(a) Take into account:

(A) Ways in which consumers normally interact with the controller;

(B) A need for security and reliability in communications related to the request; and

(C) The controller's ability to authenticate the identity of the consumer that makes the request; and

(b) Provide a clear and conspicuous link to a webpage where the consumer or an authorized agent may opt out from a controller's processing of the consumer's personal data as described in section 3 (1)(d) of this 2023 Act or, solely if the controller does not have a capacity needed for linking to a webpage, provide another method the consumer can use to opt out.

(6) If a consumer or authorized agent uses a method described in subsection (5) of this section to opt out of a controller's processing of the consumer's personal data under section 3 (1)(d) of this 2023 Act and the decision conflicts with a consumer's voluntary participation in a bona fide reward, club card or loyalty program or a program that provides premium features or discounts in return for the consumer's consent to the controller's processing of the consumer's personal data, the controller may either comply with the request to opt out or notify the consumer of the conflict and ask the consumer to affirm that the consumer intends to withdraw from the bona fide reward, club card or loyalty program or the program that provides premium features or discounts. If the consumer affirms that the consumer intends to withdraw, the controller shall comply with the request to opt out.

SECTION 6.

(1) A processor shall adhere to a controller's instructions and shall assist the controller in meeting the controller's obligations under sections 1 to 9 of this 2023 Act. In assisting the controller, the processor must:

(a) Enable the controller to respond to requests from consumers under section 4 of this 2023 Act by means that take into account how the processor processes personal data and the information available to the processor and that use appropriate technical and organizational measures to the extent reasonably practicable;

(b) Adopt administrative, technical and physical safeguards that are reasonably designed to protect the security and confidentiality of the personal data the processor processes, taking into account how the processor processes the personal data and the information available to the processor; and

(c) Provide information reasonably necessary for the controller to conduct and document data protection assessments.

(2) The processor shall enter into a contract with the controller that governs how the processor processes personal data on the controller's behalf. The contract must:

(a) Be valid and binding on both parties;

(b) Set forth clear instructions for processing data, the nature and purpose of the processing, the type of data that is subject to processing and the duration of the processing;

(c) Specify the rights and obligations of both parties with respect to the subject matter of the contract;

(d) Ensure that each person that processes personal data is subject to a duty of confidentiality with respect to the personal data;

(e) Require the processor to delete the personal data or return the personal data to the controller at the controller's direction or at the end of the provision of services, unless a law requires the processor to retain the personal data;

(f) Require the processor to make available to the controller, at the controller's request, all information the controller needs to verify that the processor has complied with all obligations the processor has under sections 1 to 9 of this 2023 Act;

(g) Require the processor to enter into a subcontract with a person the processor engages to assist with processing personal data on the controller's behalf and in the subcontract require the subcontractor to meet the processor's obligations under the processor's contract with the controller; and

(h) Allow the controller, the controller's designee or a qualified and independent person the processor engages, in accordance with an appropriate and accepted control standard, framework or procedure, to assess the processor's policies and technical and organizational measures for complying with the processor's obligations under sections 1 to 9 of this 2023 Act, and require the processor to cooperate with the assessment and, at the controller's request, report the results of the assessment to the controller.

(3) This section does not relieve a controller or processor from any liability that accrues under sections 1 to 9 of this 2023 Act as a result of the controller's or processor's actions in processing personal data.

(4)(a) For purposes of determining obligations under sections 1 to 9 of this 2023 Act, a person is a controller with respect to processing a set of personal data, and is subject to an action under section 9 of this 2023 Act to punish a violation of sections 1 to 9 of this 2023 Act, if the person:

(A) Does not need to adhere to another person's instructions to process the personal data;

(B) Does not adhere to another person's instructions with respect to processing the personal data when the person is obligated to do so; or

(C) Begins at any point to determine the purposes and means for processing the personal data, alone or in concert with another person.

(b) A determination under this subsection is a fact-based determination that must take account of the context in which a set of personal data is processed.

(c) A processor that adheres to a controller's instructions with respect to a specific processing of personal data remains a processor.

SECTION 7.

(1)(a) A controller that possesses deidentified data shall:

(A) Take reasonable measures to ensure that the deidentified data cannot be associated with an individual;

(B) Publicly commit to maintaining and using deidentified data without attempting to reidentify the deidentified data; and

(C) Enter into a contract with a recipient of the deidentified data and provide in the contract that the recipient must comply with the controller's obligations under sections 1 to 9 of this 2023 Act.

(b) A controller that discloses deidentified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the deidentified data is subject and shall take appropriate steps to address any breaches of the contractual commitments.

(c) This section does not prohibit a controller from attempting to reidentify deidentified data solely for the purpose of testing the controller's methods for deidentifying data.

(2) Sections 1 to 9 of this 2023 Act do not:

(a) Require a controller or processor to:

(A) Reidentify deidentified data; or

(B) Associate a consumer with personal data in order to authenticate the consumer's request under section 4 of this 2023 Act by:

(i) Maintaining data in identifiable form; or

(ii) Collecting, retaining or accessing any particular data or technology.

(b) Require a controller or processor to comply with a consumer's request under section 4 of this 2023 Act if the controller:

(A)Cannot reasonably associate the request with personal data or if the controller's attempt to associate the request with personal data would be unreasonably burdensome;

(B) Does not use personal data to recognize or respond to the specific consumer who is the subject of the personal data or associate the personal data with any other personal data about the specific consumer; and

(C) Does not sell or otherwise voluntarily disclose personal data to a third party, except as otherwise provided in this section.

SECTION 8.

(1)(a) A controller shall conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer.

(b) Processing activities that present a heightened risk of harm to a consumer include:

(A) Processing personal data for the purpose of targeted advertising;

(B) Processing sensitive data;

(C) Selling personal data; and

(D) Using the personal data for purposes of profiling, if the profiling presents a reasonably foreseeable risk of:

(i) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;

(ii) Financial, physical or reputational injury to consumers;

(iii) Physical or other types of intrusion upon a consumer's solitude, seclusion or private affairs or concerns, if the intrusion would be offensive to a reasonable person; or

(iv) Other substantial injury to consumers.

(c) A single data protection assessment may address a comparable set of processing operations that present a similar heightened risk of harm.

(2) A data protection assessment shall identify and weigh how processing personal data may directly or indirectly benefit the controller, the consumer, other stakeholders and the public against potential risks to the consumer, taking into account how safeguards the controller employs can mitigate the risks. In conducting the assessment, the controller shall consider how deidentified data might reduce risks, the reasonable expectations of consumers, the context in which the data is processed and the relationship between the controller and the consumers whose personal data the controller will process.

(3) The Attorney General may require a controller to provide to the Attorney General any data protection assessments the controller has conducted if the data protection assessment is relevant to an investigation the Attorney General conducts under section 9 of this 2023 Act. The Attorney General may evaluate a data protection assessment for the controller's compliance with the requirements of section 1 to 9 of this 2023 Act. If a data protection assessment the Attorney General obtains under this subsection includes information that is subject to attorney-client privilege or is work product that is subject to a privilege, the controller's provision of the data protection assessment does not waive the privilege.

(4) A data protection assessment that a controller conducts to comply with another applicable law or regulation satisfies the requirements of this section if the data protection assessment is reasonably similar in scope and effect to a data protection assessment conducted under this section.

(5) Requirements that apply to a data protection assessment under this section apply only to processing activities that occur on and after July 1, 2024, and are not retroactive.

(6) A controller shall retain for at least five years all data protection assessments the controller conducts under this section.

(7) A data protection assessment is confidential and is not subject to disclosure under ORS 192.311 to 192.478.

SECTION 9.

(1)(a) The Attorney General may serve an investigative demand upon any person that possesses, controls or has custody of any information, document or other material that the Attorney General determines is relevant to an investigation of a violation of sections 1 to 9 of this 2023 Act or that could lead to a discovery of relevant information. An investigative demand may require the person to:

(A) Appear and testify under oath at the time and place specified in the investigative demand;

(B) Answer written interrogatories; or

(C) Produce relevant documents or physical evidence for examination at the time and place specified in the investigative demand.

(b) The Attorney General shall serve an investigative demand under this section in the manner provided in ORS 646.622. The Attorney General may enforce the investigative demand as provided in ORS 646.626.

(2)(a) An attorney may accompany, represent and advise in confidence a person that appears in response to a demand under subsection (1)(a)(A) of this section. The person may refuse to answer any question on constitutional grounds or on the basis of any other legal right or privilege, including protection against self-incrimination, but must answer any other question that is not subject to the right or privilege. If the person refuses to answer a question on grounds that the answer would be self-incriminating, the Attorney General may compel the person to testify as provided in ORS 136.617.

(b) The Attorney General shall exclude from the place in which the Attorney General conducts an examination under this subsection all persons other than the person the Attorney General is examining, the person's attorney, the officer before which the person gives the testimony and any stenographer recording the testimony.

(3)(a) The Attorney General shall hold in confidence and may not disclose to any person any documents, including data protection assessments, answers to interrogatories and transcripts of oral testimony, except that the Attorney General may disclose the documents to:

(A) The person that provided the documents or the oral testimony;

(B) The attorney or representative of the person that provided the documents or oral testimony;

(C) Employees of the Attorney General; or

(D) An official of the United States or of any state who is authorized to enforce federal or state consumer protection laws if the Attorney General first obtains a written agreement from the official in which the official agrees to abide by the confidentiality requirements of this subsection.

(b) The Attorney General may use any of the materials described in paragraph (a) of this subsection in any investigation the Attorney General conducts under this section or in any action or proceeding the Attorney General brings or initiates in a court or before an administrative agency in connection with the investigation.

(4)(a) The Attorney General may bring an action to seek a civil penalty of not more than $7,500 for each violation of sections 1 to 9 of this 2023 Act or to enjoin a violation or obtain other equitable relief. The Attorney General shall bring the action in the circuit court for Multnomah County or the circuit court of a county where any part of the violation occurred.

(b) A court may award reasonable attorney fees, expert witness fees and costs of investigation to the Attorney General if the Attorney General prevails in an action under this subsection. The court may award reasonable attorney fees to a defendant that prevails in an action under this subsection if the court finds that the Attorney General had no objectively reasonable basis for asserting the claim or for appealing an adverse decision of the trial court.

(c) The Attorney General shall deposit the proceeds of any recovery under this subsection into the Department of Justice Protection and Education Revolving Account, as provided in ORS 180.095.

(5) Before bringing an action under subsection (4) of this section, the Attorney General shall notify a controller of a violation of sections 1 to 9 of this 2023 Act if the Attorney General determines that the controller can cure the violation. If the controller fails to cure the violation within 30 days after receiving the notice of the violation, the Attorney General may bring the action without further notice.

(6) The Attorney General shall bring an action under subsection (4) of this section within five years after the date of the last act of a controller that constituted the violation for which the Attorney General seeks relief.

(7) The remedies available to the Attorney General under subsection (4) of this section are in addition to and not in lieu of any other relief available to the Attorney General or another person under other applicable provisions of law. A claim available under another provision of law may be joined to the Attorney General's claim under subsection (4) of this section.

(8) The Attorney General has exclusive authority to enforce the provisions of sections 1 to 9 of this 2023 Act. Sections 1 to 9 of this 2023 Act, or any other laws of this state, do not create a private right of action to enforce a violation of sections 1 to 9 of this 2023 Act.

SECTION 10.

ORS 180.095 is amended to read:

180.095. (1) The Department of Justice Protection and Education Revolving Account is created in the General Fund. All moneys in the account are continuously appropriated to the Department of Justice and may be used to pay for only the following activities:

(a) Restitution and refunds in proceedings described in paragraph (c) of this subsection;

(b) Consumer and business education relating to the laws governing antitrust and unlawful trade practices; and

(c) Personal services, travel, meals, lodging and all other costs and expenses incurred by the department in investigating, preparing, commencing and prosecuting the following actions and suits, and enforcing judgments, settlements, compromises and assurances of voluntary compliance arising out of the following actions and suits:

(A) Actions and suits under the state and federal antitrust laws;

(B) Actions and suits under ORS 336.184 and 646.605 to 646.656;

(C) Actions commenced under ORS 59.331; [and]

(D) Actions and suits under ORS 180.750 to 180.785[.]; and

(E) Actions commenced under section 9 of this 2023 Act.

(2) Moneys in the Department of Justice Protection and Education Revolving Account are not subject to allotment. Upon request of the Attorney General, the State Treasurer shall create sub- accounts within the account for the purposes of managing moneys in the account and allocating those moneys to the activities described in subsection (1) of this section.

(3) Except as otherwise provided by law, all sums of money received by the Department of Justice under a judgment, settlement, compromise or assurance of voluntary compliance, including damages, restitution, refunds, attorney fees, costs, disbursements and other recoveries, but excluding civil penalties under ORS 646.642, in proceedings described in subsection (1)(c) of this section shall, upon receipt, be deposited with the State Treasurer to the credit of the Department of Justice Protection and Education Revolving Account. However, if the action or suit was based on an expenditure or loss from a public body or a dedicated fund, the amount of such expenditure or loss, after deduction of attorney fees and expenses awarded to the department by the court or agreed to by the parties, if any, shall be credited to the public body or dedicated fund and the remainder thereof credited to the Department of Justice Protection and Education Revolving Account.

(4) If the Department of Justice recovers restitution or refunds in a proceeding described in subsection (1)(c) of this section, and the department cannot determine the persons to whom the restitution or refunds should be paid or the amount of the restitution or refund payable to individual claimants is de minimis, the restitution or refunds may not be deposited in the Department of Justice Protection and Education Revolving Account and shall be deposited in the General Fund.

(5) Before April 1 of each odd-numbered year, the Department of Justice shall report to the Joint Committee on Ways and Means:

(a) The department's projection of the balance in the Department of Justice Protection and Education Revolving Account at the end of the biennium in which the report is made and at the end of the following biennium;

(b) The amount of the balance held for restitution and refunds; Enrolled Senate Bill 619 (SB 619-B) Page 14

(c) An estimate of the department's anticipated costs and expenses under subsection (1)(b) and

(d) of this section for the biennium in which the report is made and for the following biennium; and

(e) Any judgment, settlement, compromise or other recovery, the proceeds of which are used for purposes other than:

(A) For deposit into the Department of Justice Protection and Education Revolving Account; or

(B) For payment of legal costs related to the judgment, settlement, compromise or other recovery.

(6) The Joint Committee on Ways and Means, after consideration of recommendations made by the Department of Justice, shall use the information reported under subsection (5) of this section to determine an appropriate balance for the revolving account.

SECTION 11.

Section 9 of this 2023 Act is amended to read:

Sec. 9. (1)(a) The Attorney General may serve an investigative demand upon any person that possesses, controls or has custody of any information, document or other material that the Attorney General determines is relevant to an investigation of a violation of sections 1 to 9 of this 2023 Act or that could lead to a discovery of relevant information. An investigative demand may require the person to:

(A) Appear and testify under oath at the time and place specified in the investigative demand;

(B) Answer written interrogatories; or

(C) Produce relevant documents or physical evidence for examination at the time and place specified in the investigative demand.

(b) The Attorney General shall serve an investigative demand under this section in the manner provided in ORS 646.622. The Attorney General may enforce the investigative demand as provided in ORS 646.626.

(2)(a) An attorney may accompany, represent and advise in confidence a person that appears in response to a demand under subsection (1)(a)(A) of this section. The person may refuse to answer any question on constitutional grounds or on the basis of any other legal right or privilege, including protection against self-incrimination, but must answer any other question that is not subject to the right or privilege. If the person refuses to answer a question on grounds that the answer would be self-incriminating, the Attorney General may compel the person to testify as provided in ORS 136.617.

(b) The Attorney General shall exclude from the place in which the Attorney General conducts an examination under this subsection all persons other than the person the Attorney General is examining, the person's attorney, the officer before which the person gives the testimony and any stenographer recording the testimony.

(3)(a) The Attorney General shall hold in confidence and may not disclose to any person any documents, including data protection assessments, answers to interrogatories and transcripts of oral testimony, except that the Attorney General may disclose the documents to:

(A) The person that provided the documents or the oral testimony;

(B) The attorney or representative of the person that provided the documents or oral testimony;

(C) Employees of the Attorney General; or

(D) An official of the United States or of any state who is authorized to enforce federal or state consumer protection laws if the Attorney General first obtains a written agreement from the official in which the official agrees to abide by the confidentiality requirements of this subsection.

(b) The Attorney General may use any of the materials described in paragraph (a) of this subsection in any investigation the Attorney General conducts under this section or in any action or proceeding the Attorney General brings or initiates in a court or before an administrative agency in connection with the investigation.

(4)(a) The Attorney General may bring an action to seek a civil penalty of not more than $7,500 for each violation of sections 1 to 9 of this 2023 Act or to enjoin a violation or obtain other equi- table relief. The Attorney General shall bring the action in the circuit court for Multnomah County or the circuit court of a county where any part of the violation occurred.

(b) A court may award reasonable attorney fees, expert witness fees and costs of investigation to the Attorney General if the Attorney General prevails in an action under this subsection. The court may award reasonable attorney fees to a defendant that prevails in an action under this subsection if the court finds that the Attorney General had no objectively reasonable basis for asserting the claim or for appealing an adverse decision of the trial court.

(c) The Attorney General shall deposit the proceeds of any recovery under this subsection into the Department of Justice Protection and Education Revolving Account, as provided in ORS 180.095.

[(5) Before bringing an action under subsection (4) of this section, the Attorney General shall notify a controller of a violation of sections 1 to 9 of this 2023 Act if the Attorney General determines that the controller can cure the violation. If the controller fails to cure the violation within 30 days after receiving the notice of the violation, the Attorney General may bring the action without further notice.]

[(6)] (5) The Attorney General shall bring an action under subsection (4) of this section within five years after the date of the last act of a controller that constituted the violation for which the Attorney General seeks relief.

[(7)] (6) The remedies available to the Attorney General under subsection (4) of this section are in addition to and not in lieu of any other relief available to the Attorney General or another person under other applicable provisions of law. A claim available under another provision of law may be joined to the Attorney General's claim under subsection (4) of this section.

[(8)] (7) The Attorney General has exclusive authority to enforce the provisions of sections 1 to 9 of this 2023 Act. Sections 1 to 9 of this 2023 Act, or any other laws of this state, do not create a private right of action to enforce a violation of sections 1 to 9 of this 2023 Act.

SECTION 12. Section 5 of this 2023 Act is amended to read:

Sec. 5. (1) A controller shall:

(a) Specify in the privacy notice described in subsection (4) of this section the express purposes for which the controller is collecting and processing personal data;

(b) Limit the controller's collection of personal data to only the personal data that is adequate, relevant and reasonably necessary to serve the purposes the controller specified in paragraph (a) of this subsection;

(c) Establish, implement and maintain for personal data the same safeguards described in ORS 646A.622 that are required for protecting personal information, as defined in ORS 646A.602, such that the controller's safeguards protect the confidentiality, integrity and accessibility of the personal data to the extent appropriate for the volume and nature of the personal data; and

(d) Provide an effective means by which a consumer may revoke consent a consumer gave under sections 1 to 9 of this 2023 Act to the controller's processing of the consumer's personal data. The means must be at least as easy as the means by which the consumer provided consent. Once the consumer revokes consent, the controller shall cease processing the personal data as soon as is practicable, but not later than 15 days after receiving the revocation.

(2) A controller may not:

(a) Process personal data for purposes that are not reasonably necessary for and compatible with the purposes the controller specified in subsection (1)(a) of this section, unless the controller obtains the consumer's consent;

(b) Process sensitive data about a consumer without first obtaining the consumer's consent or, if the controller knows the consumer is a child, without processing the sensitive data in accordance with the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501 et seq. and the regulations, rules and guidance adopted under the Act, all as in effect on the effective date of this 2023 Act;

(c) Process a consumer's personal data for the purposes of targeted advertising, of profiling the consumer in furtherance of decisions that produce legal effects or effects of similar significance or of selling the consumer's personal data without the consumer's consent if the controller has actual knowledge that, or willfully disregards whether, the consumer is at least 13 years of age and not older than 15 years of age; or

(d) Discriminate against a consumer that exercises a right provided to the consumer under sections 1 to 9 of this 2023 Act by means such as denying goods or services, charging different prices or rates for goods or services or providing a different level of quality or selection of goods or services to the consumer.

(3) Subsections (1) and (2) of this section do not:

(a) Require a controller to provide a good or service that requires personal data from a consumer that the controller does not collect or maintain; or

(b) Prohibit a controller from offering a different price, rate, level of quality or selection of goods or services to a consumer, including an offer for no fee or charge, in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discount or club card program.

(4) A controller shall provide to consumers a reasonably accessible, clear and meaningful privacy notice that:

(a) Lists the categories of personal data, including the categories of sensitive data, that the controller processes;

(b) Describes the controller's purposes for processing the personal data;

(c) Describes how a consumer may exercise the consumer's rights under sections 1 to 9 of this 2023 Act, including how a consumer may appeal a controller's denial of a consumer's request under section 4 of this 2023 Act;

(d) Lists all categories of personal data, including the categories of sensitive data, that the controller shares with third parties;

(e) Describes all categories of third parties with which the controller shares personal data at a level of detail that enables the consumer to understand what type of entity each third party is and, to the extent possible, how each third party may process personal data;

(f) Specifies an electronic mail address or other online method by which a consumer can contact the controller that the controller actively monitors;

(g) Identifies the controller, including any business name under which the controller registered with the Secretary of State and any assumed business name that the controller uses in this state;

(h) Provides a clear and conspicuous description of any processing of personal data in which the controller engages for the purpose of targeted advertising or for the purpose of profiling the consumer in furtherance of decisions that produce legal effects or effects of similar significance, and a procedure by which the consumer may opt out of this type of processing; and

(i) Describes the method or methods the controller has established for a consumer to submit a request under section 4 (1) of this 2023 Act.

(5) The method or methods described in subsection (4)(i) of this section for submitting a consumer's request to a controller must:

(a) Take into account:

(A) Ways in which consumers normally interact with the controller;

(B) A need for security and reliability in communications related to the request; and

(C) The controller's ability to authenticate the identity of the consumer that makes the request; [and]

(b) Provide a clear and conspicuous link to a webpage where the consumer or an authorized agent may opt out from a controller's processing of the consumer's personal data as described in section 3 (1)(d) of this 2023 Act or, solely if the controller does not have a capacity needed for linking to a webpage, provide another method the consumer can use to opt out[.]; and

(c) Allow a consumer or authorized agent to send a signal to the controller that indicates the consumer's preference to opt out of the sale of personal data or targeted advertising under section 3 (1)(d) of this 2023 Act by means of a platform, technology or mechanism that:

(A) Does not unfairly disadvantage another controller;

(B) Does not use a default setting but instead requires the consumer or authorized agent to make an affirmative, voluntary and unambiguous choice to opt out;

(C) Is consumer friendly and easy for an average consumer to use;

(D) Is as consistent as possible with similar platforms, technologies or mechanisms required under federal or state laws or regulations; and

(E) Enables the controller to accurately determine whether the consumer is a resident of this state and has made a legitimate request under section 4 of this 2023 Act to opt out as described in section 3 (1)(d) of this 2023 Act.

(6) If a consumer or authorized agent uses a method described in subsection (5) of this section to opt out of a controller's processing of the consumer's personal data under section 3 (1)(d) of this 2023 Act and the decision conflicts with a consumer's voluntary participation in a bona fide reward, club card or loyalty program or a program that provides premium features or discounts in return for the consumer's consent to the controller's processing of the consumer's personal data, the controller may either comply with the request to opt out or notify the consumer of the conflict and ask the consumer to affirm that the consumer intends to withdraw from the bona fide reward, club card or loyalty program or the program that provides premium features or discounts. If the consumer affirms that the consumer intends to withdraw, the controller shall comply with the request to opt out.

SECTION 13.

Sections 1 to 9 of this 2023 Act do not apply before July 1, 2025, to the activities of an organization described in section 501(c)(3) of the Internal Revenue Code that is exempt from income tax under section 501(a) of the Internal Revenue Code.

SECTION 14.

Notwithstanding any other law limiting expenditures, the limitation on expenditures established by section 2 (3), chapter , Oregon Laws 2023 (Enrolled Senate Bill 5514), for the biennium beginning July 1, 2023, as the maximum limit for payment of expenses from fees, moneys or other revenues, including Miscellaneous Receipts, but excluding lottery funds and federal funds, collected or received by the Department of Justice for the Civil Enforcement Division, is increased by $1,780,729 for the purpose of carrying out the provisions of this 2023 Act.

SECTION 15.

(1) Sections 1 to 9 of this 2023 Act and the amendments to ORS 180.095 by section 10 of this 2023 Act become operative on July 1, 2024.

(2) The amendments to section 5 of this 2023 Act by section 12 of this 2023 Act become operative on January 1, 2026.

(3) The amendments to section 9 of this 2023 Act by section 11 of this 2023 Act become operative on January 1, 2026.

Tennessee Information Protection Act

SECTION 1.

This act is known and may be cited as the "Tennessee Information Protection Act."

SECTION 2.

Tennessee Code Annotated, Title 47, Chapter 18, is amended by adding the following as a new part:

47-18-3201. Part definitions.

As used in this part:

(1) "Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity or shares common branding with another legal entity. As used in this subdivision (1), "control" or "controlled" means:

(A) Ownership of, or the power to vote, more than fifty percent (50%) of the outstanding shares of a class of voting security of a company;

(B) Control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or

(C) The power to exercise controlling influence over the management of a company;

(2) "Authenticate" means to verify using reasonable means that a consumer who is entitled to exercise the rights in § 47-18-3203, is the same consumer who is exercising those consumer rights with respect to the personal information at issue;

(3) "Biometric data":

(A) Means data generated by automatic measurement of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retina or iris, or other unique biological patterns or characteristics that are used to identify a specific individual; and

(B) Does not include a physical or digital photograph, video recording, or audio recording or data generated from a photograph or video or audio recording; or information collected, used, or stored for healthcare treatment, payment, or operations under HIPAA;

(4) "Business associate" has the same meaning as defined by HIPAA;

(5) "Child" means a natural person younger than thirteen (13) years of age;

(6) "Consent":

(A) Means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal information relating to the consumer; and

(B) May include a written statement, including a statement written by electronic means, or an unambiguous affirmative action;

(7) "Consumer":

(A) Means a natural person who is a resident of this state acting only in a personal context; and

(B) Does not include a natural person acting in a commercial or employment context;

(8) "Controller" means the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal information;

(9) "Covered entity" has the same meaning as defined by HIPAA;

(10) "Decisions that produce legal or similarly significant effects concerning the consumer" means decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, healthcare services, or access to basic necessities, such as food and water;

(11) "De-identified data" means data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to that individual;

(12) "Health record":

(A) Means a written, printed, or electronically recorded material that:

(i) Was created or is maintained by a healthcare entity described in or licensed under title 68 in the course of providing healthcare services to an individual; and

(ii) Concerns the individual and the services provided; and

(B) Includes the substance of a communication made by an individual to a healthcare entity described in or licensed under title 68 in confidence during or in connection with the provision of healthcare services or information otherwise acquired by the healthcare entity about an individual in confidence and in connection with the provision of healthcare services to the individual;

(13) "HIPAA" means the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d et seq.);

(14) "Identified or identifiable natural person," "natural person," and "individual" mean a human being who can be readily identified, whether directly or indirectly;

(15) "Institution of higher education" means a public or private institution of higher education;

(16) "Nonprofit organization" means:

(A) A corporation organized under the Tennessee Nonprofit Corporation Act, compiled in title 48, chapter 51;

(B) An organization exempt from taxation under the Internal Revenue Code, codified in 26 U.S.C. §§ 501-530;

(C) A public utility organized under the laws of this state; or

(D) An entity owned or controlled by a nonprofit organization;

(17) “Personal information”:

(A) Means information that is linked or reasonably linkable to an identified or identifiable natural person; and

(B) Does not include information that is:

(i) Publicly available information; or

(ii) De-identified or aggregate consumer information;

(18) “Precise geolocation data”:

(A) Means information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of a natural person with precision and accuracy within a radius of one thousand seven hundred fifty feet (1,750’); and

(B) Does not include:

(i) The content of communications; or

(ii) Data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility;

(19) “Process” or “processing” means an operation or set of operations performed, whether by manual or automated means, on personal information or on sets of personal information, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal information;

(20) “Processor” means a natural or legal entity that processes personal information on behalf of a controller;

(21) “Profiling” means a form of solely automated processing performed on personal information to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person’s economic situation, health, personal preferences, interests, reliability, behavior, location, or movements;

(22) “Protected health information” has the same meaning as defined by HIPAA;

(23) “Pseudonymous data” means personal information that cannot be attributed to a specific natural person without the use of additional information, so long as the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable natural person;

(24) “Publicly available information” means information that is lawfully made available through federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience;

(25) “Sale of personal information”:

(A) Means the exchange of personal information for valuable monetary consideration by the controller to a third party; and

(B) Does not include:

(i) The disclosure of personal information to a processor that processes the personal information on behalf of the controller;

(ii) The disclosure of personal information to a third party for purposes of providing a product or service requested by the consumer;

(iii) The disclosure or transfer of personal information to an affiliate of the controller;

(iv) The disclosure of information that the consumer:

(a) Intentionally made available to the general public via a channel of mass media; and

(b) Did not restrict to a specific audience; or

(v) The disclosure or transfer of personal information to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets;

(26) "Sensitive data" means a category of personal information that includes:

(A) Personal information revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;

(B) The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;

(C) The personal information collected from a known child; or

(D) Precise geolocation data;

(27) "State agency" means an agency, institution, board, bureau, commission, council, or instrumentality of state government in the executive branch;

(28) "Targeted advertising":

(A) Means displaying to a consumer an advertisement that is selected based on personal information obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests; and

(B) Does not include:

(i) Advertisements based on activities within a controller's own websites or online applications;

(ii) Advertisements based on the context of a consumer's current search query, visit to a website, or online application;

(iii) Advertisements directed to a consumer in response to the consumer's request for information or feedback; or

(iv) Personal information processed solely for measuring or reporting advertising performance, reach, or frequency;

(29) "Third party" means a natural or legal person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller; and

(30) "Trade secret" means information, without regard to form, including, but not limited to, technical, nontechnical, or financial data, a formula, pattern, compilation, program, device, method, technique, plan, or process, that:

(A) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from the information's disclosure or use; and

(B) Is the subject of efforts that are reasonable under the circumstances to maintain the information's secrecy.

47-18-3202. Scope.

This part applies to persons that conduct business in this state producing products or services that target residents of this state and that:

(1) Exceed twenty-five million dollars ($25,000,000) in revenue; and

(2)

(A) Control or process personal information of at least twenty-five thousand (25,000) consumers and derive more than fifty percent (50%) of gross revenue from the sale of personal information; or

(B) During a calendar year, control or process personal information of at least one hundred seventy-five thousand (175,000) consumers.

47-18-3203. Personal information rights – Consumers.

(a)

(1) A consumer may invoke the consumer rights authorized pursuant to subdivision (a)(2) at any time by submitting a request to a controller specifying the consumer rights the consumer wishes to invoke. A known child's parent or legal guardian may invoke the consumer rights authorized pursuant to subdivision (a)(2) on behalf of the child regarding processing personal information belonging to the known child.

(2) A controller shall comply with an authenticated consumer request to exercise the right to:

(A) Confirm whether a controller is processing the consumer's personal information and to access the personal information;

(B) Correct inaccuracies in the consumer's personal information, taking into account the nature of the personal information and the purposes of the processing of the consumer's personal information;

(C) Delete personal information provided by or obtained about the consumer. A controller is not required to delete information that it maintains or uses as aggregate or de-identified data; provided, that such data in the possession of the controller is not linked to a specific consumer. A controller that obtained personal information about a consumer from a source other than the consumer is in compliance with a consumer's request to delete such personal information by:

(i)

(a) Retaining a record of the deletion request and the minimum information necessary for the purpose of ensuring that the consumer's personal information remains deleted from the controller's records; and

(b) Not using such retained personal information for any purpose prohibited under this part; or

(ii) Opting the consumer out of the processing of such personal data for any purpose except for those exempted under this part;

(D) Obtain a copy of the consumer's personal information that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means; or

(E) Opt out of a controller's processing of personal information for purposes of:

(i) Selling personal information about the consumer;

(ii) Targeted advertising; or

(iii) Profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

(b) Except as otherwise provided in this part, a controller shall comply with an authenticated request by a consumer to exercise the consumer rights authorized pursuant to subdivision (a)(2) as follows:

(1) A controller shall respond to the consumer without undue delay, but in all cases within forty-five (45) days of receipt of a request submitted pursuant to subsection (a). The response period may be extended once by forty-five (45) additional days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of the extension within the initial forty-five-day response period, together with the reason for the extension;

(2) If a controller declines to take action regarding the consumer's request, then the controller shall inform the consumer without undue delay, but in all cases and at the latest within forty-five (45) days of receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision pursuant to subsection (c);

(3) Information provided in response to a consumer request must be provided by a controller free of charge, up to twice annually per consumer. If requests from a consumer are manifestly unfounded, technically infeasible, excessive, or repetitive, then the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, technically infeasible, excessive, or repetitive nature of the request; and

(4) If a controller is unable to authenticate the request using commercially reasonable efforts, then the controller is not required to comply with a request to initiate an action under subsection (a) and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.

(c) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision pursuant to subdivision (b)(2). The appeal process must be made available to the consumer in a conspicuous manner, must be available at no cost to the consumer, and must be similar to the process for submitting requests to initiate action pursuant to subsection (a). Within sixty (60) days of receipt of an appeal, a controller shall inform the consumer in writing of action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, then the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general and reporter to submit a complaint.

47-18-3204. Data controller responsibilities – Transparency.

(a) A controller shall:

(1) Limit the collection of personal information to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer;

(2) Except as otherwise provided in this part, not process personal information for purposes that are beyond what is reasonably necessary to and compatible with the disclosed purposes for which the personal information is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;

(3) Establish, implement, and maintain reasonable administrative, technical, and physical data security practices, as described in § 47-18-3213, to protect the confidentiality, integrity, and accessibility of personal information. The data security practices must be appropriate to the volume and nature of the personal information at issue;

(4) Not be required to delete information that it maintains or uses as aggregate or de-identified data, provided that such data in the possession of the business is not linked to a specific consumer;

(5) Not process personal information in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising the consumer rights contained in this part, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer. However, this subdivision (a)(5) does not require a controller to provide a product or service that requires the personal information of a consumer that the controller does not collect or maintain, or prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised the right to opt out pursuant to § 47-18-3203(a)(2)(F) or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program; and

(6) Not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing the data in accordance with the federal Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.) and its implementing regulations.

(b) A provision of a contract or agreement that purports to waive or limit the consumer rights described in § 47-18-3203 is contrary to public policy and is void and unenforceable.

(c) A controller shall provide a reasonably accessible, clear, and meaningful privacy notice that includes:

(1) The categories of personal information processed by the controller;

(2) The purpose for processing personal information;

(3) How consumers may exercise their consumer rights pursuant to § 47-18-3203, including how a consumer may appeal a controller's decision with regard to the consumer's request;

(4) The categories of personal information that the controller sells to third parties, if any; and

(5) The categories of third parties, if any, to whom the controller sells personal information.

(d) If a controller sells personal information to third parties or processes personal information for targeted advertising, then the controller shall clearly and conspicuously disclose the processing, as well as the manner in which a consumer may exercise the right to opt out of the processing.

(e)

(1) A controller shall provide, and shall describe in a privacy notice, one (1) or more secure and reliable means for a consumer to submit a request to exercise the consumer rights in § 47-18-3203. Such means must take into account the:

(A) Ways in which a consumer normally interacts with the controller;

(B) Need for secure and reliable communication of such requests; and

(C) Ability of a controller to authenticate the identity of the consumer making the request.

(2) A controller shall not require a consumer to create a new account in order to exercise consumer rights in § 47-18-3203, but may require a consumer to use an existing account.

47-18-3205. Responsibility according to role – Controller and processor.

(a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under this part. The assistance must include:

(1) Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as this is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests pursuant to § 47-18-3203; and

(2) Providing necessary information to enable the controller to conduct and document data protection assessments pursuant to § 47-18-3206.

(b) A contract between a controller and a processor governs the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract is binding and must clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract must also include requirements that the processor shall:

(1) Ensure that each person processing personal information is subject to a duty of confidentiality with respect to the data;

(2) At the controller's direction, delete or return all personal information to the controller as requested at the end of the provision of services, unless retention of the personal information is required by law;

(3) Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this part;

(4) Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this part using an appropriate and accepted control standard or framework and assessment procedure for the assessments. The processor shall provide a report of each assessment to the controller upon request; and

(5) Engage a subcontractor pursuant to a written contract in that requires the subcontractor to meet the obligations of the processor with respect to the personal information.

(c) This section does not relieve a controller or a processor from the liabilities imposed on it by virtue of its role in the processing relationship as described in subsection (b).

(d) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal information is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal information remains a processor.

47-18-3206. Data protection assessments.

(a) A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal information:

(1) The processing of personal information for purposes of targeted advertising;

(2) The sale of personal information;

(3) The processing of personal information for purposes of profiling, where the profiling presents a reasonably foreseeable risk of:

(A) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;

(B) Financial, physical, or reputational injury to consumers;

(C) A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where the intrusion would be offensive to a reasonable person; or

(D) Other substantial injury to consumers;

(4) The processing of sensitive data; and

(5) Processing activities involving personal information that present a heightened risk of harm to consumers.

(b) Data protection assessments conducted pursuant to subsection (a) must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards that can be employed by the controller to reduce the risks. The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal information will be processed, must be factored into this assessment by the controller.

(c) The attorney general and reporter may request pursuant to a civil investigative demand that a controller disclose a data protection assessment that is relevant to an investigation conducted by the attorney general and reporter, and the controller shall make the data protection assessment available to the attorney general and reporter. The attorney general and reporter may evaluate the data protection assessment for compliance with the responsibilities set forth in § 47-18-3204. Data protection assessments are confidential and not open to public inspection and copying. The disclosure of a data protection assessment pursuant to a request from the attorney general and reporter does not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and information contained in the assessment.

(d) A single data protection assessment may address a comparable set of processing operations that include similar activities.

(e) Data protection assessments conducted by a controller for the purpose of compliance with other laws, rules, or regulations may comply with this section if the assessments have a reasonably comparable scope and effect.

(f) Data protection assessment requirements apply to processing activities created or generated on or after July 1, 2024, and are not retroactive.

47-18-3207. Processing de-identified data – Exemptions.

(a) The controller in possession of de-identified data shall:

(1) Take reasonable measures to ensure that the data cannot be associated with a natural person;

(2) Publicly commit to maintaining and using de-identified data without attempting to reidentify the data; and

(3) Contractually obligate recipients of the de-identified data to comply with this part.

(b) This section does not require a controller or processor to:

(1) Reidentify de-identified data or pseudonymous data;

(2) Maintain data in identifiable form, or collect, obtain, retain, or access data or technology, in order to be capable of associating an authenticated consumer request with personal information; or

(3) Comply with an authenticated consumer rights request, pursuant to § 47-18-3203, if:

(A) The controller is not reasonably capable of associating the request with the personal information or it would be unreasonably burdensome for the controller to associate the request with the personal information;

(B) The controller does not use the personal information to recognize or respond to the specific consumer who is the subject of the personal information, or associate the personal information with other personal information about the same specific consumer; and

(C) The controller does not sell the personal information to a third party or otherwise voluntarily disclose the personal information to a third party other than a processor, except as otherwise permitted in this section.

(c) The consumer rights contained in §§ 47-18-3203 and 47-18-3204 do not apply to pseudonymous data in cases where the controller is able to demonstrate information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing that information.

(d) A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address breaches of those contractual commitments.

47-18-3208. Limitations.

(a) This part does not restrict a controller's or processor's ability to:

(1) Comply with federal, state, or local laws, rules, or regulations;

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

(3) Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;

(4) Investigate, establish, exercise, prepare for, or defend legal claims;

(5) Provide a product or service specifically requested by a consumer or the parent or legal guardian of a known child, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer prior to entering into a contract;

(6) Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis;

(7) Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activity, or illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for such action;

(8) Engage in public- or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, or similar independent oversight entity that determines whether:

(A) Deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller;

(B) The expected benefits of the research outweigh the privacy risks; and

(C) The controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including risks associated with reidentification; or

(9) Assist another controller, processor, or third party with the obligations under this part.

(b) The obligations imposed on controllers or processors under this part do not restrict a controller's or processor's ability to collect, use, or retain data to:

(1) Conduct internal research to develop, improve, or repair products, services, or technology;

(2) Effectuate a product recall;

(3) Identify and repair technical errors that impair existing or intended functionality; or

(4) Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

(c) The obligations imposed on controllers or processors under this part do not apply where compliance by the controller or processor with this part would violate an evidentiary privilege under the laws of this state. This part does not prevent a controller or processor from providing personal information concerning a consumer to a person covered by an evidentiary privilege under the laws of this state as part of a privileged communication.

(d)

(1) A controller or processor that discloses personal information to a third-party controller or processor, in compliance with the requirements of this part, is not in violation of this part if:

(A) The third-party controller or processor that receives and processes the personal information is in violation of this part; and

(B) At the time of disclosing the personal information, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation.

(2) A third-party controller or processor receiving personal information from a controller or processor in compliance with the requirements of this part is likewise not in violation of this part for the violations of the controller or processor from which it receives such personal information.

(e) This part does not impose an obligation on controllers and processors that adversely affects the rights or freedoms of a person, such as exercising the right of free speech pursuant to the First Amendment to the United States Constitution, or applies to the processing of personal information by a person in the course of a purely personal activity.

(f) A controller shall not process personal information for purposes other than those expressly listed in this section unless otherwise allowed by this part. Personal information processed by a controller pursuant to this section may be processed to the extent that the processing is:

(1) Reasonably necessary and proportionate to the purposes listed in this section; and

(2) Adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section. Personal information collected, used, or retained pursuant to subsection (b) shall, where applicable, take into account the nature and purpose or purposes of the collection, use, or retention. The data is subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal information and to reduce reasonably foreseeable risks of harm to consumers relating to the collection, use, or retention of personal information.

(g) If a controller processes personal information pursuant to an exemption in this section, then the controller bears the burden of demonstrating that the processing qualifies for the exemption and complies with subsection (f).

(h) Processing personal information for the purposes expressly identified in subdivisions (a)(1)-(9) does not solely make an entity a controller with respect to the processing.

47-18-3209. Investigative authority.

If the attorney general and reporter has reasonable cause to believe that an individual, controller, or processor has engaged in, is engaging in, or is about to engage in a violation of this part, then the attorney general and reporter may issue a civil investigative demand.

47-18-3210. Exemptions.

(a) This part does not apply to:

(1) A body, authority, board, bureau, commission, district, or agency of this state or of a political subdivision of this state;

(2) A financial institution, an affiliate of a financial institution, or data subject to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.);

(3) An individual, firm, association, corporation, or other entity that is licensed in this state under title 56 as an insurance company and transacts insurance business;

(4) A covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States department of health and human services, 45 CFR Parts 160 and 164 established pursuant to HIPAA, and the federal Health Information Technology for Economic and Clinical Health Act (P.L. 111-5);

(5) A nonprofit organization;

(6) An institution of higher education;

(7) Protected health information under HIPAA;

(8) Health records for purposes of title 68;

(9) Patient identifying information for purposes of 42 U.S.C. § 290dd-2;

(10) Personal information:

(A) Processed for purposes of:

(i) Research conducted in accordance with the federal policy for the protection of human subjects under 45 CFR Part 46;

(ii) Human subjects research conducted in accordance with good clinical practice guidelines issued by The International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use; or

(iii) Research conducted in accordance with the protection of human subjects under 21 CFR Parts 6, 50, and 56; or

(B) Processed or sold in connection with research conducted in accordance with the requirements set forth in this part, or other research conducted in accordance with applicable law;

(11) Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986 (42 U.S.C. § 11101 et seq.);

(12) Patient safety work product for purposes of the federal Patient Safety and Quality Improvement Act (42 U.S.C. § 299b-21 et seq.);

(13) Information that is:

(A) Derived from the healthcare-related information listed in this subsection (a) that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA; or

(B) Included in a limited data set as described in 45 CFR 164.514(e), to the extent that the information is used, disclosed, and maintained in the manner specified in 45 CFR 164.514(e);

(14) Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this subsection (a) that is maintained by a covered entity or business associate as defined by HIPAA or a program or a qualified service organization as defined by 42 U.S.C. § 290dd-2;

(15) Information used only for public health activities and purposes as authorized by HIPAA;

(16) The collection, maintenance, disclosure, sale, communication, or use of personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency or furnisher that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the federal Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.);

(17) Personal information collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. § 2721 et seq.);

(18) Personal information or educational information regulated by the federal Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g et seq.);

(19) Personal information collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act (12 U.S.C. § 2001 et seq.);

(20) Data processed or maintained:

(A) In the course of an individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role;

(B) As the emergency contact information of an individual under this part used for emergency contact purposes; or

(C) That is necessary to retain to administer benefits for another individual relating to the individual under subdivision (a)(20)(A) and used for the purposes of administering those benefits;

(21) Information collected as part of public- or peer-reviewed scientific or statistical research in the public interest;

(22) An insurance producer licensed under title 56; or

(23) Personal information maintained or used for purposes of compliance with the regulation of listed chemicals under the federal Controlled Substances Act (21 U.S.C. § 830).

(b) Controllers and processors that comply with the verifiable parental consent requirements of the federal Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.) are deemed compliant with an obligation to obtain parental consent under this part.

(c) This part does not require a controller, processor, third party, or consumer to disclose trade secrets.

47-18-3211. Contracts.

(a) A provision of a contract or agreement that waives or limits a consumer's rights under this part, including, but not limited to, a right to a remedy or means of enforcement, is contrary to public policy, void, and unenforceable.

(b) This part does not prevent a consumer from declining to request information from a controller, declining to opt out of a controller's sale of the consumer's personal information, or authorizing a controller to sell the consumer's personal information after previously opting out.

(c) This part applies to contracts entered into, amended, or renewed on or after the effective date of this act.

47-18-3212. Enforcement – Civil penalty – Expenses.

(a) The attorney general and reporter has exclusive authority to enforce this part.

(b) The attorney general and reporter may develop reasonable cause to believe that a controller or processor is in violation of this part, based on the attorney general and reporter's own inquiry or on consumer or public complaints. Prior to initiating an action under this part, the attorney general and reporter shall provide a controller or processor sixty-days' written notice identifying the specific provisions of this part the attorney general and reporter alleges have been or are being violated. If within the sixty-day period, the controller or processor cures the noticed violation and provides the attorney general and reporter an express written statement that the alleged violations have been cured and that no such further violations shall occur, then the attorney general and reporter shall not initiate an action against the controller or processor.

(c) If a controller or processor continues to violate this part following the cure period in subsection (b) or breaches an express written statement provided to the attorney general and reporter under subsection (b), then the attorney general and reporter may bring an action in a court of competent jurisdiction seeking any of the following relief:

(1) Declaratory judgment that the act or practice violates this chapter;

(2) Injunctive relief, including preliminary and permanent injunctions, to prevent an additional violation of and compel compliance with this part;

(3) Civil penalties, as described in subsection (d);

(4) Reasonable attorney's fees and investigative costs; or

(5) Other relief the court determines appropriate.

(d)

(1) A court may impose a civil penalty of up to seven thousand five hundred dollars ($7,500) for each violation of this part.

(2) If the court finds the controller or processor willfully or knowingly violated this part, then the court may, in its discretion, award treble damages.

(e) A violation of this part shall not serve as the basis for, or be subject to, a private right of action, including a class action lawsuit, under this part or other law.

(f) The attorney general and reporter may recover reasonable expenses incurred in investigating and preparing a case, including attorney fees, in an action initiated under this part.

47-18-3213. Affirmative defense – Voluntary privacy program.

(a) A controller or processor has an affirmative defense to a cause of action for a violation of this part if the controller or processor creates, maintains, and complies with a written privacy policy that:

(1)

(A) Reasonably conforms to the National Institute of Standards and Technology (NIST) privacy framework entitled "A Tool for Improving Privacy through Enterprise Risk Management Version 1.0." or other documented policies, standards, and procedures designed to safeguard consumer privacy; and

(B) Is updated to reasonably conform with a subsequent revision to the NIST or comparable privacy framework within two (2) years of the publication date stated in the most recent revision to the NIST or comparable privacy framework; and

(2) Provides a person with the substantive rights required by this part.

(b) The scale and scope of a controller or processor's privacy program under subsection (a) is appropriate if it is based on all of the following factors:

(1) The size and complexity of the controller or processor's business;

(2) The nature and scope of the activities of the controller or processor;

(3) The sensitivity of the personal information processed;

(4) The cost and availability of tools to improve privacy protections and data governance; and

(5) Compliance with a comparable state or federal law.

(c)

(1) In addition to subsections (a) and (b):

(A) A controller may be certified pursuant to the Asia Pacific Economic Cooperation's Cross Border Privacy Rules system; and

(B) A processor may be certified pursuant to the Asia Pacific Economic Cooperation's Privacy Recognition for Processors system.

(2) Certifications under subdivision (c)(1) may be considered in addition to the factors in subsection (b).

SECTION 3.

If a provision of this act or its application to a person or circumstance is held invalid, then the invalidity does not affect other provisions or applications of the act that can be given effect without the invalid provision or application, and to that end, the provisions of this act are severable.

SECTION 4.

This act supersedes and preempts any conflicting provisions of any public or private act and laws, ordinances, resolutions, regulations, or the equivalent adopted by a home rule municipality, county, including a metropolitan government, or city regarding the processing of personal data by controllers or processors. To the extent there exists a conflict, this section does not require the home rule municipality, county, or city to adopt any law, ordinance, resolution, regulation, or the equivalent to modify or repeal such conflicting provisions enacted prior to the effective date of this act.

SECTION 5.

The headings in this act are for reference purposes only and do not constitute a part of the law enacted by this act. However, the Tennessee Code Commission is requested to include the headings in any compilation or publication containing this act.

SECTION 6.

This act takes effect July 1, 2025, the public welfare requiring it.

Texas Data Privacy and Security Act

AN ACT

relating to the regulation of the collection, use, processing, and treatment of consumers ' personal data by certain business entities; imposing a civil penalty.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTIONA1.AAThis Act may be cited as the Texas Data Privacy and Security Act.

SECTIONA2.AATitle 11, Business & Commerce Code, is amended by adding Subtitle C to read as follows:

SUBTITLE C. CONSUMER DATA PROTECTION

CHAPTER 541. CONSUMER DATA PROTECTION

SUBCHAPTER A. GENERAL PROVISIONS

Sec. 541.001. DEFINITIONS.

In this chapter, unless a different meaning is required by the context:

(1) "Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity or shares common branding with another legal entity. For purposes of this subdivision, "control" or "controlled" means:

(A) the ownership of, or power to vote, more than 50 percent of the outstanding shares of any class of voting security of a company;

(B) the control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or

(C) the power to exercise controlling influence over the management of a company.

(2) "Authenticate" means to verify through reasonable means that the consumer who is entitled to exercise the consumer's rights under Subchapter B is the same consumer exercising those consumer rights with respect to the personal data at issue.

(3) "Biometric data" means data generated by automatic measurements of an individual 's biological characteristics. The term includes a fingerprint, voiceprint, eye retina or iris, or other unique biological pattern or characteristic that is used to identify a specific individual. The term does not include a physical or digital photograph or data generated from a physical or digital photograph, a video or audio recording or data generated from a video or audio recording, or information collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.).

(4) "Business associate" has the meaning assigned to the term by the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.).

(5) "Child" means an individual younger than 13 years of age.

(6) "Consent," when referring to a consumer, means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. The term includes a written statement, including a statement written by electronic means, or any other unambiguous affirmative action. The term does not include:

(A) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information;

(B) hovering over, muting, pausing, or closing a given piece of content; or

(C) agreement obtained through the use of dark patterns.

(7) "Consumer" means an individual who is a resident of this state acting only in an individual or household context. The term does not include an individual acting in a commercial or employment context.

(8) "Controller" means an individual or other person that, alone or jointly with others, determines the purpose and means of processing personal data.

(9) "Covered entity" has the meaning assigned to the term by the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.).

(10) "Dark pattern" means a user interface designed or manipulated with the effect of substantially subverting or impairing user autonomy, decision-making, or choice, and includes any practice the Federal Trade Commission refers to as a dark pattern.

(11) "Decision that produces a legal or similarly significant effect concerning a consumer" means a decision made by the controller that results in the provision or denial by the controller of:

(A) financial and lending services;

(B) housing, insurance, or health care services;

(C) education enrollment;

(D) employment opportunities;

(E) criminal justice; or

(F) access to basic necessities, such as food and water.

(12) "Deidentified data" means data that cannot reasonably be linked to an identified or identifiable individual, or a device linked to that individual.

(13) "Health care provider" has the meaning assigned to the term by the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.).

(14) "Health record" means any written, printed, or electronically recorded material maintained by a health care provider in the course of providing health care services to an individual that concerns the individual and the services provided. The term includes:

(A) the substance of any communication made by an individual to a health care provider in confidence during or in connection with the provision of health care services; or

(B) information otherwise acquired by the health care provider about an individual in confidence and in connection with health care services provided to the individual.

(15) "Identified or identifiable individual" means a consumer who can be readily identified, directly or indirectly.

(16) "Institution of higher education" means:

(A) an institution of higher education as defined by Section 61.003, Education Code; or

(B) a private or independent institution of higher education as defined by Section 61.003, Education Code.

(17) "Known child" means a child under circumstances where a controller has actual knowledge of, or wilfully disregards, the child's age.

(18) "Nonprofit organization" means:

(A) a corporation organized under Chapters 20 and 22, Business Organizations Code, and the provisions of Title 1, Business Organizations Code, to the extent applicable to nonprofit corporations;

(B) an organization exempt from federal taxation under Section 501(a), Internal Revenue Code of 1986, by being listed as an exempt organization under Section 501(c)(3), 501(c)(6), 501(c)(12), or 501(c)(19) of that code;

(C) a political organization; or

(D) an organization that:

(i) is exempt from federal taxation under Section 501(a), Internal Revenue Code of 1986, by being listed as an exempt organization under Section 501(c)(4) of that code; and

(ii) is described by Section 701.052(a), Insurance Code.

(19) "Personal data" means any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual. The term includes pseudonymous data when the data is used by a controller or processor in conjunction with additional information that reasonably links the data to an identified or identifiable individual. The term does not include deidentified data or publicly available information.

(20) "Political organization" means a party, committee, association, fund, or other organization, regardless of whether incorporated, that is organized and operated primarily for the purpose of influencing or attempting to influence:

(A) the selection, nomination, election, or appointment of an individual to a federal, state, or local public office or an office in a political organization, regardless of whether the individual is selected, nominated, elected, or appointed; or

(B) the election of a presidential/vice-presidential elector, regardless of whether the elector is selected, nominated, elected, or appointed.

(21) "Precise geolocation data" means information derived from technology, including global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet. The term does not include the content of communications or any data generated by or connected to an advanced utility metering infrastructure system or to equipment for use by a utility.

(22) "Process" or "processing" means an operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(23) "Processor" means a person that processes personal data on behalf of a controller.

(24) "Profiling" means any form of solely automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual 's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(25) "Protected health information" has the meaning assigned to the term by the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.).

(26) "Pseudonymous data" means any information that cannot be attributed to a specific individual without the use of additional information, provided that the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

(27) "Publicly available information" means information that is lawfully made available through government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by a consumer, or by a person to whom a consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.

(28) "Sale of personal data" means the sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party. The term does not include:

(A) the Adisclosure of personal data to a processor that processes the personal data on the controller's behalf;

(B) the Adisclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;

(C) the disclosure or transfer of personal data to an affiliate of the controller;

(D) the disclosure of information that the consumer:

(i) intentionally made available to the general public through a mass media channel; and

(ii) did not restrict to a specific audience; or

(E) theAdisclosure or transfer of personal data to a third party as an asset that is part of a merger or acquisition.

(29) "Sensitive data" means a category of personal data. The term includes:

(A) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexuality, or citizenship or immigration status;

(B) genetic or biometric data that is processed for the purpose of uniquely identifying an individual;

(C) personal data collected from a known child; or

(D) precise geolocation data.

(30) "State agency" means a department, commission, board, office, council, authority, or other agency in any branch of state government that is created by the constitution or a statute of this state, including a university system or institution of higher education as defined by Section 61.003, Education Code.

(31) "Targeted advertising" means displaying to a consumer an advertisement that is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests. The term does not include:

(A) an advertisement that:

(i) is based on activities within a controller's own websites or online applications;

(ii) is based on the context of a consumer's current search query, visit to a website, or online application; or

(iii) is directed to a consumer in response to the consumer 's request for information or feedback; or

(B) the processing of personal data solely for measuring or reporting advertising performance, reach, or frequency.

(32) "Third party" means a person, other than the consumer, the controller, the processor, or an affiliate of the controller or processor.

(33) "Trade secret" means all forms and types of information, including business, scientific, technical, economic, or engineering information, and any formula, design, prototype, pattern, plan, compilation, program device, program, code, device, method, technique, process, procedure, financial data, or list of actual or potential customers or suppliers, whether tangible or intangible and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:

(A) the owner of the trade secret has taken reasonable measures under the circumstances to keep the information secret; and

(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

Sec. 541.002. APPLICABILITY OF CHAPTER.

(a) This chapter applies only to a person that:

(1) conducts business in this state or produces a product or service consumed by residents of this state;

(2) processes or engages in the sale of personal data; and

(3) is not a small business as defined by the United States Small Business Administration, except to the extent that Section 541.107 applies to a person described by this subdivision.

(b) This chapter does not apply to:

(1) a state agency or a political subdivision of this state;

(2) a financial institution or data subject to Title V, Gramm-Leach-Bliley Act (15 U.S.C. Section 6801 et seq.);

(3) a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, 45 C.F.R. Parts 160 and 164, established under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.), and the Health Information Technology for Economic and Clinical Health Act (Division A, Title XIII, and Division B, Title IV, Pub. L. No.A111-5);

(4) a nonprofit organization;

(5) an institution of higher education; or

(6) an electric utility, a power generation company, or a retail electric provider, as those terms are defined by Section 31.002, Utilities Code.

Sec. 541.003. CERTAIN INFORMATION EXEMPT FROM CHAPTER.

The following information is exempt from this chapter:

(1) protected health information under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.);

(2) health records;

(3) patient identifying information for purposes of 42 U.S.C. Section 290dd-2;

(4) identifiable private information:

(A) for purposes of the federal policy for the protection of human subjects under 45 C.F.R. Part 46;

(B) collected as part of human subjects research under the good clinical practice guidelines issued by The International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use (ICH) or of the protection of human subjects under 21 C.F.R. Parts 50 and 56; or

(C) that is personal data used or shared in research conducted in accordance with the requirements set forth in this chapter or other research conducted in accordance with applicable law;

(5) information and documents created for purposes of the Health Care Quality Improvement Act of 1986 (42 U.S.C. Section 11101 et seq.);

(6) patient safety work product for purposes of the Patient Safety and Quality Improvement Act of 2005 (42 U.S.C. Section 299b-21 et seq.);

(7) information derived from any of the health care-related information listed in this section that is deidentified in accordance with the requirements for deidentification under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.);

(8) information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this section that is maintained by a covered entity or business associate as defined by the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.) or by a program or a qualified service organization as defined by 42 U.S.C. Section 290dd-2;

(9) information that is included in a limited data set as described by 45 C.F.R. Section 164.514(e), to the extent that the information is used, disclosed, and maintained in the manner specified by 45 C.F.R. Section 164.514(e);

(10) information collected or used only for public health activities and purposes as authorized by the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.);

(11) the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency or furnisher that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that the activity is regulated by and authorized under the Fair Credit Reporting Act (15 U.S.C. Section 1681 et seq.);

(12) personal data collected, processed, sold, or disclosed in compliance with the Driver 's Privacy Protection Act of 1994 (18 U.S.C. Section 2721 et seq.);

(13) personal data regulated by the Family Educational Rights and Privacy Act of 1974 (20 U.S.C. Section 1232g);

(14) personal data collected, processed, sold, or disclosed in compliance with the Farm Credit Act of 1971 (12 U.S.C. Section 2001 et seq.);

(15) data processed or maintained in the course of an individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role;

(16) data processed or maintained as the emergency contact information of an individual under this chapter that is used for emergency contact purposes; or

(17) data that is processed or maintained and is necessary to retain to administer benefits for another individual that relates to an individual described by Subdivision (15) and used for the purposes of administering those benefits.

Sec. 541.004. INAPPLICABILITY OF CHAPTER.

This chapter does not apply to the processing of personal data by a person in the course of a purely personal or household activity.

Sec. 541.005. EFFECT OF COMPLIANCE WITH PARENTAL CONSENT REQUIREMENTS UNDER CERTAIN FEDERAL LAW.

A controller or processor that complies with the verifiable parental consent requirements of the Children 's Online Privacy Protection Act of 1998 (15 U.S.C. Section 6501 et seq.) with respect to data collected online is considered to be in compliance with any requirement to obtain parental consent under this chapter.

SUBCHAPTER B. CONSUMER 'S RIGHTS

Sec. 541.051. CONSUMER 'S PERSONAL DATA RIGHTS; REQUEST TO EXERCISE RIGHTS.

(a) A consumer is entitled to exercise the consumer rights authorized by this section at any time by submitting a request to a controller specifying the consumer rights the consumer wishes to exercise. With respect to the processing of personal data belonging to a known child, a parent or legal guardian of the child may exercise the consumer rights on behalf of the child.

(b) A controller shall comply with an authenticated consumer request to exercise the right to:

(1) confirm whether a controller is processing the consumer 's personal data and to access the personal data;

(2) correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer 's personal data;

(3) delete personal data provided by or obtained about the consumer;

(4) if the data is available in a digital format, obtain a copy of the consumer 's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance; or

(5) opt out of the processing of the personal data for purposes of:

(A) targeted advertising;

(B) the sale of personal data; or

(C) profiling in furtherance of a decision that produces a legal or similarly significant effect concerning the consumer.

Sec. 541.052. CONTROLLER RESPONSE TO CONSUMER REQUEST.

(a) Except as otherwise provided by this chapter, a controller shall comply with a request submitted by a consumer to exercise the consumer 's rights pursuant to Section 541.051 as provided by this section.

(b) A controller shall respond to the consumer request without undue delay, which may not be later than the 45th day after the date of receipt of the request. The controller may extend the response period once by an additional 45 days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of the extension within the initial 45-day response period, together with the reason for the extension.

(c) If a controller declines to take action regarding the consumer 's request, the controller shall inform the consumer without undue delay, which may not be later than the 45th day after the date of receipt of the request, of the justification for declining to take action and provide instructions on how to appeal the decision in accordance with Section 541.053.

(d) A controller shall provide information in response to a consumer request free of charge, at least twice annually per consumer. If a request from a consumer is manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or may decline to act on the request. The controller bears the burden of demonstrating for purposes of this subsection that a request is manifestly unfounded, excessive, or repetitive.

(e) If a controller is unable to authenticate the request using commercially reasonable efforts, the controller is not required to comply with a consumer request submitted under Section 541.051 and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.

(f) A controller that has obtained personal data about a consumer from a source other than the consumer is considered in compliance with a consumer 's request to delete that personal data pursuant to Section 541.051(b)(3) by:

(1) retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer 's personal data remains deleted from the business 's records and not using the retained data for any other purpose under this chapter; or

(2) opting the consumer out of the processing of that personal data for any purpose other than a purpose that is exempt under the provisions of this chapter.

Sec. 541.053. APPEAL.

(a) A controller shall establish a process for a consumer to appeal the controller 's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision under Section 541.052(c).

(b) The appeal process must be conspicuously available and similar to the process for initiating action to exercise consumer rights by submitting a request under Section 541.051.

(c) A controller shall inform the consumer in writing of any action taken or not taken in response to an appeal under this section not later than the 60th day after the date of receipt of the appeal, including a written explanation of the reason or reasons for the decision.

(d) If the controller denies an appeal, the controller shall provide the consumer with the online mechanism described by Section 541.152 through which the consumer may contact the attorney general to submit a complaint.

Sec. 541.054. WAIVER OR LIMITATION OF CONSUMER RIGHTS PROHIBITED.

Any provision of a contract or agreement that waives or limits in any way a consumer right described by Sections 541.051, 541.052, and 541.053 is contrary to public policy and is void and unenforceable.

Sec. 541.055. METHODS FOR SUBMITTING CONSUMER REQUESTS.

(a) A controller shall establish two or more secure and reliable methods to enable consumers to submit a request to exercise their consumer rights under this chapter. The methods must take into account:

(1) the ways in which consumers normally interact with the controller;

(2) the necessity for secure and reliable communications of those requests; and

(3) the ability of the controller to authenticate the identity of the consumer making the request.

(b) A controller may not require a consumer to create a new account to exercise the consumer 's rights under this subchapter but may require a consumer to use an existing account.

(c) Except as provided by Subsection (d), if the controller maintains an Internet website, the controller must provide a mechanism on the website for consumers to submit requests for information required to be disclosed under this chapter.

(d) A controller that operates exclusively online and has a direct relationship with a consumer from whom the controller collects personal information is only required to provide an e-mail address for the submission of requests described by Subsection (c).

(e) A consumer may designate another person to serve as the consumer 's authorized agent and act on the consumer 's behalf to opt out of the processing of the consumer 's personal data under Sections 541.051(b)(5)(A) and (B). A consumer may designate an authorized agent using a technology, including a link to an Internet website, an Internet browser setting or extension, or a global setting on an electronic device, that allows the consumer to indicate the consumer 's intent to

opt out of the processing. A controller shall comply with an opt-out request received from an authorized agent under this subsection if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent 's authority to act on the consumer's behalf. A controller is not required to comply with an opt-out request received from an authorized agent under this subsection if:

(1) the authorized agent does not communicate the request to the controller in a clear and unambiguous manner;

(2) the controller is not able to verify, with commercially reasonable effort, that the consumer is a resident of this state;

(3) the controller does not possess the ability to process the request; or

(4) the controller does not process similar or identical requests the controller receives from consumers for the purpose of complying with similar or identical laws or regulations of another state.

(f) A technology described by Subsection (e):

(1) may not unfairly disadvantage another controller;

(2) may not make use of a default setting, but must require the consumer to make an affirmative, freely given, and unambiguous choice to indicate the consumer 's intent to opt out of any processing of a consumer 's personal data; and

(3) must be consumer-friendly and easy to use by the average consumer.

SUBCHAPTER C. CONTROLLER AND PROCESSOR DATA-RELATED DUTIES AND PROHIBITIONS

Sec. 541.101. CONTROLLER DUTIES; TRANSPARENCY.

(a) A controller:

(1) shall limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which that personal data is processed, as disclosed to the consumer; and

(2) for purposes of protecting the confidentiality, integrity, and accessibility of personal data, shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices that are appropriate to the volume and nature of the personal data at issue.

(b) A controller may not:

(1) except as otherwise provided by this chapter, process personal data for a purpose that is neither reasonably necessary to nor compatible with the disclosed purpose for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer 's consent;

(2) process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers;

(3) discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including by denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer; or

(4) process the sensitive data of a consumer without obtaining the consumer 's consent, or, in the case of processing the sensitive data of a known child, without processing that data in accordance with the Children's Online Privacy Protection Act of 1998 (15 U.S.C. Section 6501 et seq.).

(c) Subsection (b)(3) may not be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised the consumer 's right to opt out under Section 541.051 or the offer is related to a consumer 's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

Sec. 541.102.AAPRIVACY NOTICE.

(a) A controller shall provide consumers with a reasonably accessible and clear privacy notice that includes:

(1) the categories of personal data processed by the controller, including, if applicable, any sensitive data processed by the controller;

(2) the purpose for processing personal data;

(3) how consumers may exercise their consumer rights under Subchapter B, including the process by which a consumer may appeal a controller 's decision with regard to the consumer's request;

(4) if applicable, the categories of personal data that the controller shares with third parties;

(5) if applicable, the categories of third parties with whom the controller shares personal data; and

(6) a description of the methods required under Section 541.055 through which consumers can submit requests to exercise their consumer rights under this chapter.

(b) If a controller engages in the sale of personal data that is sensitive data, the controller shall include the following notice: "NOTICE: We may sell your sensitive personal data." The notice must be posted in the same location and in the same manner as the privacy notice described by Subsection (a).

(c) If a controller engages in the sale of personal data that is biometric data, the controller shall include the following notice: "NOTICE: We may sell your biometric personal data." The notice must be posted in the same location and in the same manner as the privacy notice described by Subsection (a).

Sec. 541.103. SALE OF DATA TO THIRD PARTIES AND PROCESSING DATA FOR TARGETED ADVERTISING; DISCLOSURE.

If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose that process and the manner in which a consumer may exercise the right to opt out of that process.

Sec. 541.104. DUTIES OF PROCESSOR.

(a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting or complying with the controller's duties or requirements under this chapter, including:

(1) assisting the controller in responding to consumer rights requests submitted under Section 541.051 by using appropriate technical and organizational measures, as reasonably practicable, taking into account the nature of processing and the information available to the processor;

(2) assisting the controller with regard to complying with the requirement relating to the security of processing personal data and to the notification of a breach of security of the processor 's system under Chapter 521, taking into account the nature of processing and the information available to the processor; and

(3) providing necessary information to enable the controller to conduct and document data protection assessments under Section 541.105.

(b) A contract between a controller and a processor shall govern the processor 's data processing procedures with respect to processing performed on behalf of the controller. The contract must include:

(1) clear instructions for processing data;

(2) the nature and purpose of processing;

(3) the type of data subject to processing;

(4) the duration of processing;

(5) the rights and obligations of both parties; and

(6) a requirement that the processor shall:

(A) ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

(B) at the controller's direction, delete or return all personal data to the controller as requested after the provision of the service is completed, unless retention of the personal data is required by law;

(C) make available to the controller, on reasonable request, all information in the processor's possession necessary to demonstrate the processor 's compliance with the requirements of this chapter;

(D) allow, and cooperate with, reasonable assessments by the controller or the controller 's designated assessor; and

(E) engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the requirements of the processor with respect to the personal data.

(c) Notwithstanding the requirement described by Subsection (b)(6)(D), a processor, in the alternative, may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the requirements under this chapter using an appropriate and accepted control standard or framework and assessment procedure. The processor shall provide a report of the assessment to the controller on request.

(d) This section may not be construed to relieve a controller or a processor from the liabilities imposed on the controller or processor by virtue of its role in the processing relationship as described by this chapter.

(e) A determination of whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends on the context in which personal data is to be processed. A processor that continues to adhere to a controller 's instructions with respect to a specific processing of personal data remains in the role of a processor.

Sec. 541.105. DATA PROTECTION ASSESSMENTS.

(a) A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data:

(1) the processing of personal data for purposes of targeted advertising;

(2) the sale of personal data;

(3) the processing of personal data for purposes of profiling, if the profiling presents a reasonably foreseeable risk of:

(A) unfair or deceptive treatment of or unlawful disparate impact on consumers;

(B) financial, physical, or reputational injury to consumers;

(C) a physical or other intrusion on the solitude or seclusion, or the private affairs or concerns, of consumers, if the intrusion would be offensive to a reasonable person; or

(D) other substantial injury to consumers;

(4) the processing of sensitive data; and

(5) any processing activities involving personal data that present a heightened risk of harm to consumers.

(b) A data protection assessment conducted under Subsection (a) must:

(1) identify and weigh the direct or indirect benefits that may flow from the processing to the controller, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, as mitigated by safeguards that can be employed by the controller to reduce the risks; and

(2) factor into the assessment:

(A) the use of deidentified data;

(B) the reasonable expectations of consumers;

(C) the context of the processing; and

(D) the relationship between the controller and the consumer whose personal data will be processed.

(c) A controller shall make a data protection assessment requested under Section 541.153(b) available to the attorney general pursuant to a civil investigative demand under Section 541.153.

(d) A data protection assessment is confidential and exempt from public inspection and copying under Chapter 552, Government Code. Disclosure of a data protection assessment in compliance with a request from the attorney general does not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

(e) A single data protection assessment may address a comparable set of processing operations that include similar activities.

(f) A data protection assessment conducted by a controller for the purpose of compliance with other laws or regulations may constitute compliance with the requirements of this section if the assessment has a reasonably comparable scope and effect.

Sec. 541.106. DEIDENTIFIED OR PSEUDONYMOUS DATA.

(a) A controller in possession of deidentified data shall:

(1) take reasonable measures to ensure that the data cannot be associated with an individual;

(2) publicly commit to maintaining and using deidentified data without attempting to reidentify the data; and

(3) contractually obligate any recipient of the deidentified data to comply with the provisions of this chapter.

(b) This chapter may not be construed to require a controller or processor to:

(1) reidentify deidentified data or pseudonymous data;

(2) maintain data in identifiable form or obtain, retain, or access any data or technology for the purpose of allowing the controller or processor to associate a consumer request with personal data; or

(3) comply with an authenticated consumer rights request under Section 541.051, if the controller:

(A) is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data;

(B) does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data or associate the personal data with other personal data about the same specific consumer; and

(C) does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted by this section.

(c) The consumer rights under Sections 541.051(b)(1)-(4) and controller duties under Section 541.101 do not apply to pseudonymous data in cases in which the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

(d) A controller that discloses pseudonymous data or deidentified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or deidentified data is subject and shall take appropriate steps to address any breach of the contractual commitments.

Sec. 541.107. REQUIREMENTS FOR SMALL BUSINESSES.

(a) A person described by Section 541.002(a)(3) may not engage in the sale of personal data that is sensitive data without receiving prior consent from the consumer.

(b) A person who violates this section is subject to the penalty under Section 541.155.

SUBCHAPTER D. ENFORCEMENT

Sec. 541.151. ENFORCEMENT AUTHORITY EXCLUSIVE.

The attorney general has exclusive authority to enforce this chapter.

Sec. 541.152. INTERNET WEBSITE AND COMPLAINT MECHANISM.

The attorney general shall post on the attorney general's Internet website:

(1) information relating to:

(A) the responsibilities of a controller under Subchapters B and C;

(B) the responsibilities of a processor under Subchapter C; and

(C) a consumer 's rights under Subchapter B; and

(2) an online mechanism through which a consumer may submit a complaint under this chapter to the attorney general.

Sec. 541.153. INVESTIGATIVE AUTHORITY.

(a) If the attorney general has reasonable cause to believe that a person has engaged in or is engaging in a violation of this chapter, the attorney general may issue a civil investigative demand. The procedures established for the issuance of a civil investigative demand under Section 15.10 apply to the same extent and manner to the issuance of a civil investigative demand under this section.

(b) The attorney general may request, pursuant to a civil investigative demand issued under Subsection (a), that a controller disclose any data protection assessment that is relevant to an investigation conducted by the attorney general. The attorney general may evaluate the data protection assessment for compliance with the requirements set forth in Sections 541.101, 541.102, and 541.103.

Sec. 541.154. NOTICE OF VIOLATION OF CHAPTER; OPPORTUNITY TO CURE.

Before bringing an action under Section 541.155, the attorney general shall notify a person in writing, not later than the 30th day before bringing the action, identifying the specific provisions of this chapter the attorney general alleges have been or are being violated. The attorney general may not bring an action against the person if:

(1) within the 30-day period, the person cures the identified violation; and

(2) the person provides the attorney general a written statement that the person:

(A) cured the alleged violation;

(B) notified the consumer that the consumer 's privacy violation was addressed, if the consumer 's contact information has been made available to the person;

(C) provided supportive documentation to show how the privacy violation was cured; and

(D) made changes to internal policies, if necessary, to ensure that no such further violations will occur.

Sec. 541.155. CIVIL PENALTY; INJUNCTION.

(a) A person who violates this chapter following the cure period described by Section 541.154 or who breaches a written statement provided to the attorney general under that section is liable for a civil penalty in an amount not to exceed $7,500 for each violation.

(b) The attorney general may bring an action in the name of this state to:

(1) recover a civil penalty under this section;

(2) restrain or enjoin the person from violating this chapter; or

(3) recover the civil penalty and seek injunctive relief.

(c) The attorney general may recover reasonable attorney's fees and other reasonable expenses incurred in investigating and bringing an action under this section.

(d) The attorney general shall deposit a civil penalty collected under this section in accordance with Section 402.007, Government Code.

Sec. 541.156. NO PRIVATE RIGHT OF ACTION.

This chapter may not be construed as providing a basis for, or being subject to, a private right of action for a violation of this chapter or any other law.

SUBCHAPTER E. CONSTRUCTION OF CHAPTER; EXEMPTIONS FOR CERTAIN USES OF CONSUMER PERSONAL DATA

Sec. 541.201. CONSTRUCTION OF CHAPTER.

(a) This chapter may not be construed to restrict a controller's or processor's ability to:

(1) comply with federal, state, or local laws, rules, or regulations;

(2) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

(3) investigate, establish, exercise, prepare for, or defend legal claims;

(4) provide a product or service specifically requested by a consumer or the parent or guardian of a child, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer before entering into a contract;

(5) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another individual and in which the processing cannot be manifestly based on another legal basis;

(6) prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity;

(7) preserve the integrity or security of systems or investigate, report, or prosecute those responsible for breaches of system security;

(8) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board or similar independent oversight entity that determines:

(A) if the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller;

(B) whether the expected benefits of the research outweigh the privacy risks; and

(C) if the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification; or

(9) assist another controller, processor, or third party with any of the requirements under this subsection.

(b) This chapter may not be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of this state as part of a privileged communication.

(c) This chapter may not be construed as imposing a requirement on controllers and processors that adversely affects the rights or freedoms of any person, including the right of free speech.

(d) This chapter may not be construed as requiring a controller, processor, third party, or consumer to disclose a trade secret.

Sec. 541.202. COLLECTION, USE, OR RETENTION OF DATA FOR CERTAIN PURPOSES.

(a) The requirements imposed on controllers and processors under this chapter may not restrict a controller's or processor's ability to collect, use, or retain data to:

(1) conduct internal research to develop, improve, or repair products, services, or technology;

(2) effect a product recall;

(3) identify and repair technical errors that impair existing or intended functionality; or

(4) perform internal operations that:

(A) are reasonably aligned with the expectations of the consumer;

(B) are reasonably anticipated based on the consumer's existing relationship with the controller; or

(C) are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

(b) A requirement imposed on a controller or processor under this chapter does not apply if compliance with the requirement by the controller or processor, as applicable, would violate an evidentiary privilege under the laws of this state.

Sec. 541.203. DISCLOSURE OF PERSONAL DATA TO THIRD-PARTY CONTROLLER OR PROCESSOR.

(a) A controller or processor that discloses personal data to a third-party controller or processor, in compliance with the requirements of this chapter, does not violate this chapter if the third-party controller or processor that receives and processes that personal data is in violation of this chapter, provided that, at the time of the data's disclosure, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation.

(b) A third-party controller or processor receiving personal data from a controller or processor in compliance with the requirements of this chapter does not violate this chapter for the transgressions of the controller or processor from which the third-party controller or processor receives the personal data.

Sec. 541.204. PROCESSING OF CERTAIN PERSONAL DATA BY CONTROLLER OR OTHER PERSON.

(a) Personal data processed by a controller under this subchapter may not be processed for any purpose other than a purpose listed in this subchapter unless otherwise allowed by this chapter. Personal data processed by a controller under this subchapter may be processed to the extent that the processing of the data is:

(1) reasonably necessary and proportionate to the purposes listed in this subchapter; and

(2) adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this subchapter.

(b) Personal data collected, used, or retained under Section 541.202(a) must, where applicable, take into account the nature and purpose of such collection, use, or retention. The personal data described by this subsection is subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to the collection, use, or retention of personal data.

(c) A controller that processes personal data under an exemption in this subchapter bears the burden of demonstrating that the processing of the personal data qualifies for the exemption and complies with the requirements of Subsections (a) and (b).

(d) The processing of personal data by an entity for the purposes described by Section 541.201 does not solely make the entity a controller with respect to the processing of the data.

Sec. 541.205. LOCAL PREEMPTION.

This chapter supersedes and preempts any ordinance, resolution, rule, or other regulation adopted by a political subdivision regarding the processing of personal data by a controller or processor.

SECTION 3. (a) The Department of Information Resources, under the management of the chief privacy officer, shall review the implementation of the requirements of Chapter 541, Business & Commerce Code, as added by this Act.

(b) Not later than September 1, 2024, the Department of Information Resources shall create an online portal available on the department 's Internet website for members of the public to provide feedback and recommend changes to Chapter 541, Business & Commerce Code, as added by this Act. The online portal must remain open for receiving feedback from the public for at least 90 days.

(c) Not later than January 1, 2025, the Department of Information Resources shall make available to the public a report detailing the status of the implementation of the requirements of Chapter 541, Business & Commerce Code, as added by this Act, and any recommendations to the legislature regarding changes to that law.

(d) This section expires September 1, 2025.

SECTION 4. Data protection assessments required to be conducted under Section 541.105, Business & Commerce Code, as added by this Act, apply only to processing activities generated after the effective date of this Act and are not retroactive.

SECTION 5. Not later than July 1, 2024, the attorney general shall post the information and online mechanism required by Section 541.152, Business & Commerce Code, as added by this Act.

SECTION 6. The provisions of this Act are hereby declared severable, and if any provision of this Act or the application of such provision to any person or circumstance is declared invalid for any reason, such declaration shall not affect the validity of the remaining portions of this Act.

SECTION 7. (a) Except as provided by Subsection (b) of this section, this Act takes effect July 1, 2024.

(b) Section 541.055(e), Business & Commerce Code, as added by this Act, takes effect January 1, 2025.

Utah Consumer Privacy Act

Part 1. General Provisions

13-61-101. Definitions.

As used in this chapter:

(1) "Account" means the Consumer Privacy Restricted Account established in Section13-61-403.

(2) "Affiliate" means an entity that:

(a) controls, is controlled by, or is under common control with another entity; or

(b) shares common branding with another entity.

(3) "Aggregated data" means information that relates to a group or category of consumers:

(a) from which individual consumer identities have been removed; and

(b) that is not linked or reasonably linkable to any consumer.

(4) "Air carrier" means the same as that term is defined in 49 U.S.C. Sec. 40102.

(5) "Authenticate" means to use reasonable means to determine that a consumer's request to exercise the rights described in Section 13-61-201 is made by the consumer who is entitled to exercise those rights.

(6) (a) "Biometric data" means data generated by automatic measurements of an individual's unique biological characteristics.

(b) "Biometric data" includes data described in Subsection (6)(a) that are generated by automatic measurements of an individual's fingerprint, voiceprint, eye retinas, irises, or any other unique biological pattern or characteristic that is used to identify a specific individual.

(c) "Biometric data" does not include:

(i) a physical or digital photograph;

(ii) a video or audio recording;

(iii) data generated from an item described in Subsection (6)(c)(i) or (ii);

(iv) information captured from a patient in a health care setting; or

(v) information collected, used, or stored for treatment, payment, or health care operations as those terms are defined in 45 C.F.R. Parts 160, 162, and 164.

(7) "Business associate" means the same as that term is defined in 45 C.F.R. Sec.160.103.

(8) "Child" means an individual younger than 13 years old.

(9) "Consent" means an affirmative act by a consumer that unambiguously indicates the consumer's voluntary and informed agreement to allow a person to process personal data related to the consumer.

(10) (a) “Consumer” means an individual who is a resident of the state acting in an individual or household context.

(b) “Consumer” does not include an individual acting in an employment or commercial context.

(11) “Control” or “controlled” as used in Subsection (2) means:

(a) ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting securities of an entity;

(b) control in any manner over the election of a majority of the directors or of the individuals exercising similar functions; or

(c) the power to exercise controlling influence of the management of an entity.

(12) “Controller” means a person doing business in the state who determines the purposes for which and the means by which personal data are processed, regardless of whether the person makes the determination alone or with others.

(13) “Covered entity” means the same as that term is defined in 45 C.F.R. Sec. 160.103.

(14) “Deidentified data” means data that:

(a) cannot reasonably be linked to an identified individual or an identifiable individual; and

(b) are possessed by a controller who:

(i) takes reasonable measures to ensure that a person cannot associate the data with an individual;

(ii) publicly commits to maintain and use the data only in deidentified form and not attempt to reidentify the data; and

(iii) contractually obligates any recipients of the data to comply with the requirements described in Subsections (14)(b)(i) and (ii).

(15) “Director” means the director of the Division of Consumer Protection.

(16) “Division” means the Division of Consumer Protection created in Section 13-2-1.

(17) “Governmental entity” means the same as that term is defined in Section 63G-2-103.

(18) “Health care facility” means the same as that term is defined in Section 26-21-2.

(19) “Health care provider” means the same as that term is defined in Section 26-21-2.

(20) “Identifiable individual” means an individual who can be readily identified, directly or indirectly.

(21) “Institution of higher education” means a public or private institution of higher education.

(22) “Local political subdivision” means the same as that term is defined in Section 11-14-102.

(23) “Nonprofit corporation” means:

(a) the same as that term is defined in Section 16-6a-102; or

(b) a foreign nonprofit corporation as defined in Section 16-6a-102.

(24) (a) "Personal data" means information that is linked or reasonably linkable to an identified individual or an identifiable individual.

(b) "Personal data" does not include deidentified data, aggregated data, or publicly available information.

(25) "Process" means an operation or set of operations performed on personal data, including collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(26) "Processor" means a person who processes personal data on behalf of a controller.

(27) "Protected health information" means the same as that term is defined in 45 C.F.R. Sec. 160.103.

(28) "Pseudonymous data" means personal data that cannot be attributed to a specific individual without the use of additional information, if the additional information is:

(a) kept separate from the consumer's personal data; and

(b) subject to appropriate technical and organizational measures to ensure that the personal data are not attributable to an identified individual or an identifiable individual.

(29) "Publicly available information" means information that a person:

(a) lawfully obtains from a record of a governmental entity;

(b) reasonably believes a consumer or widely distributed media has lawfully made available to the general public; or

(c) if the consumer has not restricted the information to a specific audience, obtains from a person to whom the consumer disclosed the information.

(30) "Right" means a consumer right described in Section 13-61-201.

(31) (a) "Sale," "sell," or "sold" means the exchange of personal data for monetary consideration by a controller to a third party.

(b) "Sale," "sell," or "sold" does not include:

(i) a controller's disclosure of personal data to a processor who processes the personal data on behalf of the controller;

(ii) a controller's disclosure of personal data to an affiliate of the controller;

(iii) considering the context in which the consumer provided the personal data to the controller, a controller's disclosure of personal data to a third party if the purpose is consistent with a consumer's reasonable expectations;

(iv) the disclosure or transfer of personal data when a consumer directs a controller to:

(A) disclose the personal data; or

(B) interact with one or more third parties;

(v) a consumer's disclosure of personal data to a third party for the purpose of providing a product or service requested by the consumer or a parent or legal guardian of a child;

(vi) the disclosure of information that the consumer:

(A) intentionally makes available to the general public via a channel of mass media; and

(B) does not restrict to a specific audience; or

(vii) a controller's transfer of personal data to a third party as an asset that is part of a proposed or actual merger, an acquisition, or a bankruptcy in which the third party assumes control of all or part of the controller's assets.

(32) (a) "Sensitive data" means:

(i) personal data that reveals:

(A) an individual's racial or ethnic origin;

(B) an individual's religious beliefs;

(C) an individual's sexual orientation;

(D) an individual's citizenship or immigration status; or

(E) information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional;

(ii) the processing of genetic personal data or biometric data, if the processing is for the purpose of identifying a specific individual; or

(iii) specific geolocation data.

(b) "Sensitive data" does not include personal data that reveals an individual's:

(i) racial or ethnic origin, if the personal data are processed by a video communication service; or

(ii) if the personal data are processed by a person licensed to provide health care under Title 26, Chapter 21, Health Care Facility Licensing and Inspection Act, or Title 58, Occupations and Professions, information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional.

(33) (a) "Specific geolocation data" means information derived from technology, including global position system level latitude and longitude coordinates, that directly identifies an individual's specific location, accurate within a radius of 1,750 feet or less.

(b) "Specific geolocation data" does not include:

(i) the content of a communication; or

(ii) any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(34) (a) "Targeted advertising" means displaying an advertisement to a consumer where the advertisement is selected based on personal data obtained from the consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests.

(b) "Targeted advertising" does not include advertising:

(i) based on a consumer's activities within a controller's website or online application or any affiliated website or online application;

(ii) based on the context of a consumer's current search query or visit to a website or online application;

(iii) directed to a consumer in response to the consumer's request for information, product, a service, or feedback; or

(iv) processing personal data solely to measure or report advertising:

(A) performance;

(B) reach; or

(C) frequency.

(35) "Third party" means a person other than:

(a) the consumer, controller, or processor; or

(b) an affiliate or contractor of the controller or the processor.

(36) "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(a) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from the information's disclosure or use; and

(b) is the subject of efforts that are reasonable under the circumstances to maintain the information's secrecy.

13-61-102. Applicability.

(1) This chapter applies to any controller or processor who:

(a) (i) conducts business in the state; or

(ii) produces a product or service that is targeted to consumers who are residents of the state;

(b) has annual revenue of $25,000,000 or more; and

(c) satisfies one or more of the following thresholds:

(i) during a calendar year, controls or processes personal data of 100,000 or more consumers; or

(ii) derives over 50% of the entity's gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more consumers.

(2) This chapter does not apply to:

(a) a governmental entity or a third party under contract with a governmental entity when the third party is acting on behalf of the governmental entity;

(b) a tribe;

(c) an institution of higher education;

(d) a nonprofit corporation;

(e) a covered entity;

(f) a business associate;

(g) information that meets the definition of:

(i) protected health information for purposes of the federal Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. Sec. 1320d et seq., and related regulations;

(ii) patient identifying information for purposes of 42 C.F.R. Part 2;

(iii) identifiable private information for purposes of the Federal Policy for the Protection of Human Subjects, 45 C.F.R. Part 46;

(iv) identifiable private information or personal data collected as part of human subjects research pursuant to or under the same standards as:

(A) the good clinical practice guidelines issued by the International Council for Harmonisation; or

(B) the Protection of Human Subjects under 21 C.F.R. Part 50 and Institutional Review Boards under 21 C.F.R. Part 56;

(v) personal data used or shared in research conducted in accordance with one or more of the requirements described in Subsection (2)(g)(iv);

(vi) information and documents created specifically for, and collected and maintained by, a committee listed in Section 26-1-7;

(vii) information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, 42 U.S.C. Sec. 11101 et seq., and related regulations;

(viii) patient safety work product for purposes of 42 C.F.R. Part 3; or

(ix) information that is:

(A) deidentified in accordance with the requirements for deidentification set forth in 45 C.F.R. Part 164; and

(B) derived from any of the health care-related information listed in this Subsection (2)(g);

(h) information originating from, and intermingled to be indistinguishable with, information under Subsection (2)(g) that is maintained by:

(i) a health care facility or health care provider; or

(ii) a program or a qualified service organization as defined in 42 C.F.R. Sec. 2.11;

(i) information used only for public health activities and purposes as described in 45 C.F.R. Sec. 164.512;

(j) (i) an activity by:

(A) a consumer reporting agency, as defined in 15 U.S.C. Sec. 1681a;

(B) a furnisher of information, as set forth in 15 U.S.C. Sec. 1681s-2, who provides information for use in a consumer report, as defined in 15 U.S.C. Sec. 1681a; or

(C) a user of a consumer report, as set forth in 15 U.S.C. Sec. 1681b;

(ii) subject to regulation under the federal Fair Credit Reporting Act, 15 U.S.C. Sec. 1681 et seq.; and

(iii) involving the collection, maintenance, disclosure, sale, communication, or use of any personal data bearing on a consumer's:

(A) credit worthiness;

(B) credit standing;

(C) credit capacity;

(D) character;

(E) general reputation;

(F) personal characteristics; or

(G) mode of living;

(k) a financial institution or an affiliate of a financial institution governed by, or personal data collected, processed, sold, or disclosed in accordance with, Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. Sec. 6801 et seq., and related regulations;

(l) personal data collected, processed, sold, or disclosed in accordance with the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. Sec. 2721 et seq.;

(m) personal data regulated by the federal Family Education Rights and Privacy Act, 20 U.S.C. Sec. 1232g, and related regulations;

(n) personal data collected, processed, sold, or disclosed in accordance with the federal Farm Credit Act of 1971, 12 U.S.C. Sec. 2001 et seq.;

(o) data that are processed or maintained:

(i) in the course of an individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent the collection and use of the data are related to the individual's role;

(ii) as the emergency contact information of an individual described in Subsection (2)(o)(i) and used for emergency contact purposes; or

(iii) to administer benefits for another individual relating to an individual described in Subsection (2)(o)(i) and used for the purpose of administering the benefits;

(p) an individual's processing of personal data for purely personal or household purposes; or

(q) an air carrier.

(3) A controller is in compliance with any obligation to obtain parental consent under this chapter if the controller complies with the verifiable parental consent mechanisms under the Children's Online Privacy Protection Act, 15 U.S.C. Sec. 6501 et seq., and the act's implementing regulations and exemptions.

(4) This chapter does not require a person to take any action in conflict with the federal Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. Sec. 1320d et seq., or related regulations.

13-61-103. Preemption -- Reference to other laws.

(1) This chapter supersedes and preempts any ordinance, resolution, rule, or other regulation adopted by a local political subdivision regarding the processing of personal data by a controller or processor.

(2) Any reference to federal law in this chapter includes any rules or regulations promulgated under the federal law.

Part 2. Rights Relating to Personal Data

13-61-201. Consumer rights -- Access -- Deletion -- Portability -- Opt out of certain processing.

(1) A consumer has the right to:

(a) confirm whether a controller is processing the consumer's personal data; and

(b) access the consumer's personal data.

(2) A consumer has the right to delete the consumer's personal data that the consumer provided to the controller.

(3) A consumer has the right to obtain a copy of the consumer's personal data, that the consumer previously provided to the controller, in a format that:

(a) to the extent technically feasible, is portable;

(b) to the extent practicable, is readily usable; and

(c) allows the consumer to transmit the data to another controller without impediment, where the processing is carried out by automated means.

(4) A consumer has the right to opt out of the processing of the consumer's personal data for purposes of:

(a) targeted advertising; or

(b) the sale of personal data.

(5) Nothing in this section requires a person to cause a breach of security system as defined in Section 13-44-102.

13-61-202. Exercising consumer rights.

(1) A consumer may exercise a right by submitting a request to a controller, by means prescribed by the controller, specifying the right the consumer intends to exercise.

(2) In the case of processing personal data concerning a known child, the parent or legal guardian of the known child shall exercise a right on the child's behalf.

(3) In the case of processing personal data concerning a consumer subject to guardianship, conservatorship, or other protective arrangement under Title 75, Chapter 5, Protection of Persons Under Disability and Their Property, the guardian or the conservator of the consumer shall exercise a right on the consumer's behalf.

13-61-203. Controller's response to requests.

(1) Subject to the other provisions of this chapter, a controller shall comply with a consumer's request under Section 13-61-202 to exercise a right.

(2) (a) Within 45 days after the day on which a controller receives a request to exercise a right, the controller shall:

(i) take action on the consumer's request; and

(ii) inform the consumer of any action taken on the consumer's request.

(b) The controller may extend once the initial 45-day period by an additional 45 days if reasonably necessary due to the complexity of the request or the volume of the requests received by the controller.

(c) If a controller extends the initial 45-day period, before the initial 45-day period expires, the controller shall:

(i) inform the consumer of the extension, including the length of the extension; and

(ii) provide the reasons the extension is reasonably necessary as described in Subsection (2)(b).

(d) The 45-day period does not apply if the controller reasonably suspects the consumer's request is fraudulent and the controller is not able to authenticate the request before the 45-day period expires.

(3) If, in accordance with this section, a controller chooses not to take action on a consumer's request, the controller shall within 45 days after the day on which the controller receives the request, inform the consumer of the reasons for not taking action.

(4) (a) A controller may not charge a fee for information in response to a request, unless the request is the consumer's second or subsequent request during the same 12-month period.

(b) (i) Notwithstanding Subsection (4)(a), a controller may charge a reasonable fee to cover the administrative costs of complying with a request or refuse to act on a request, if:

(A) the request is excessive, repetitive, technically infeasible, or manifestly unfounded;

(B) the controller reasonably believes the primary purpose in submitting the request was something other than exercising a right; or

(C) the request, individually or as part of an organized effort, harasses, disrupts, or imposes undue burden on the resources of the controller's business.

(ii) A controller that charges a fee or refuses to act in accordance with this Subsection (4)(b) bears the burden of demonstrating the request satisfied one or more of the criteria described in Subsection (4)(b)(i).

(5) If a controller is unable to authenticate a consumer request to exercise a right described in Section 13-61-201 using commercially reasonable efforts, the controller:

(a) is not required to comply with the request; and

(b) may request that the consumer provide additional information reasonably necessary to authenticate the request.

Part 3. Requirements for Controllers and Processors

13-61-301. Responsibility according to role.

(1) A processor shall:

(a) adhere to the controller's instructions; and

(b) taking into account the nature of the processing and information available to the processor, by appropriate technical and organizational measures, insofar as reasonably practicable, assist the controller in meeting the controller's obligations, including obligations related to the security of processing personal data and notification of a breach of security system described in Section 13-44-202.

(2) Before a processor performs processing on behalf of a controller, the processor and controller shall enter into a contract that:

(a) clearly sets forth instructions for processing personal data, the nature and purpose of the processing, the type of data subject to processing, the duration of the processing, and the parties' rights and obligations;

(b) requires the processor to ensure each person processing personal data is subject to a duty of confidentiality with respect to the personal data; and

(c) requires the processor to engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the same obligations as the processor with respect to the personal data.

(3) (a) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data are to be processed.

(b) A processor that adheres to a controller's instructions with respect to a specific processing of personal data remains a processor.

13-61-302. Responsibilities of controllers -- Transparency -- Purpose specification and data minimization -- Consent for secondary use -- Security -- Nondiscrimination --Nonretaliation -- Nonwaiver of consumer rights.

(1) (a) A controller shall provide consumers with a reasonably accessible and clear privacy notice that includes:

(i) the categories of personal data processed by the controller;

(ii) the purposes for which the categories of personal data are processed;

(iii) how consumers may exercise a right;

(iv) the categories of personal data that the controller shares with third parties, if any; and

(v) the categories of third parties, if any, with whom the controller shares personal data.

(b) If a controller sells a consumer's personal data to one or more third parties or engages in targeted advertising, the controller shall clearly and conspicuously disclose to the consumer the manner in which the consumer may exercise the right to opt out of the:

(i) sale of the consumer's personal data; or

(ii) processing for targeted advertising.

(2) (a) A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices designed to:

(i) protect the confidentiality and integrity of personal data; and

(ii) reduce reasonably foreseeable risks of harm to consumers relating to the processing of personal data.

(b) Considering the controller's business size, scope, and type, a controller shall use data security practices that are appropriate for the volume and nature of the personal data at issue.

(3) Except as otherwise provided in this chapter, a controller may not process sensitive data collected from a consumer without:

(a) first presenting the consumer with clear notice and an opportunity to opt out of the processing; or

(b) in the case of the processing of personal data concerning a known child, processing the data in accordance with the federal Children's Online Privacy Protection Act, 15 U.S.C. Sec. 6501 et seq., and the act's implementing regulations and exemptions.

(4) (a) A controller may not discriminate against a consumer for exercising a right by:

(i) denying a good or service to the consumer;

(ii) charging the consumer a different price or rate for a good or service; or

(iii) providing the consumer a different level of quality of a good or service.

(b) This Subsection (4) does not prohibit a controller from offering a different price, rate, level, quality, or selection of a good or service to a consumer, including offering a good or service for no fee or at a discount, if:

(i) the consumer has opted out of targeted advertising; or

(ii) the offer is related to the consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

(5) A controller is not required to provide a product, service, or functionality to a consumer if:

(a) the consumer's personal data are or the processing of the consumer's personal data is reasonably necessary for the controller to provide the consumer the product, service, or functionality; and

(b) the consumer does not:

(i) provide the consumer's personal data to the controller; or

(ii) allow the controller to process the consumer's personal data.

(6) Any provision of a contract that purports to waive or limit a consumer's right under this chapter is void.

13-61-303. Processing deidentified data or pseudonymous data.

(1) The provisions of this chapter do not require a controller or processor to:

(a) reidentify deidentified data or pseudonymous data;

(b) maintain data in identifiable form or obtain, retain, or access any data or technology for the purpose of allowing the controller or processor to associate a consumer request with personal data; or

(c) comply with an authenticated consumer request to exercise a right described in Subsections 13-61-202(1) through (3), if:

(i) (A) the controller is not reasonably capable of associating the request with the personal data; or

(B) it would be unreasonably burdensome for the controller to associate the request with the personal data;

(ii) the controller does not:

(A) use the personal data to recognize or respond to the consumer who is the subject of the personal data; or

(B) associate the personal data with other personal data about the consumer; and

(iii) the controller does not sell or otherwise disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.

(2) The rights described in Subsections 13-61-201(1) through (3) do not apply to pseudonymous data if a controller demonstrates that any information necessary to identify a consumer is kept:

(a) separately; and

(b) subject to appropriate technical and organizational measures to ensure the personal data are not attributed to an identified individual or an identifiable individual.

(3) A controller who uses pseudonymous data or deidentified data shall take reasonable steps to ensure the controller:

(a) complies with any contractual obligations to which the pseudonymous data or deidentified data are subject; and

(b) promptly addresses any breach of a contractual obligation described in Subsection (3)(a).

13-61-304. Limitations.

(1) The requirements described in this chapter do not restrict a controller's or processor's ability to:

(a) comply with a federal, state, or local law, rule, or regulation;

(b) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, state, local, or other governmental entity;

(c) cooperate with a law enforcement agency concerning activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;

(d) investigate, establish, exercise, prepare for, or defend a legal claim;

(e) provide a product or service requested by a consumer or a parent or legal guardian of a child;

(f) perform a contract to which the consumer or the parent or legal guardian of a child is a party, including fulfilling the terms of a written warranty or taking steps at the request of the consumer or parent or legal guardian before entering into the contract with the consumer;

(g) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another individual;

(h) (i) detect, prevent, protect against, or respond to a security incident, identity theft, fraud, harassment, malicious or deceptive activity, or any illegal activity; or

(ii) investigate, report, or prosecute a person responsible for an action described in Subsection (1)(h)(i);

(i) (i) preserve the integrity or security of systems; or

(ii) investigate, report, or prosecute a person responsible for harming or threatening the integrity or security of systems, as applicable;

(j) if the controller discloses the processing in a notice described in Section 13-61-302, engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws;

(k) assist another person with an obligation described in this subsection;

(l) process personal data to:

(i) conduct internal analytics or other research to develop, improve, or repair a controller's or processor's product, service, or technology;

(ii) identify and repair technical errors that impair existing or intended functionality; or

(iii) effectuate a product recall;

(m) process personal data to perform an internal operation that is:

(i) reasonably aligned with the consumer's expectations based on the consumer's existing relationship with the controller; or

(ii) otherwise compatible with processing to aid the controller or processor in providing a product or service specifically requested by a consumer or a parent or legal guardian of a child or the performance of a contract to which the consumer or a parent or legal guardian of a child is a party; or

(n) retain a consumer's email address to comply with the consumer's request to exercise a right.

(2) This chapter does not apply if a controller's or processor's compliance with this chapter:

(a) violates an evidentiary privilege under Utah law;

(b) as part of a privileged communication, prevents a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under Utah law; or

(c) adversely affects the privacy or other rights of any person.

(3) A controller or processor is not in violation of this chapter if:

(a) the controller or processor discloses personal data to a third party controller or processor in compliance with this chapter;

(b) the third party processes the personal data in violation of this chapter; and

(c) the disclosing controller or processor did not have actual knowledge of the third party's intent to commit a violation of this chapter.

(4) If a controller processes personal data under an exemption described in Subsection (1), the controller bears the burden of demonstrating that the processing qualifies for the exemption.

(5) Nothing in this chapter requires a controller, processor, third party, or consumer to disclose a trade secret.

13-61-305. No private cause of action.

A violation of this chapter does not provide a basis for, nor is a violation of this chapter subject to, a private right of action under this chapter or any other law.

Part 4. Enforcement

13-61-401. Investigative powers of division.

(1) The division shall establish and administer a system to receive consumer complaints regarding a controller's or processor's alleged violation of this chapter.

(2) (a) The division may investigate a consumer complaint to determine whether the controller or processor violated or is violating this chapter.

(b) If the director has reasonable cause to believe that substantial evidence exists that a person identified in a consumer complaint is in violation of this chapter, the director shall refer the matter to the attorney general.

(c) Upon request, the division shall provide consultation and assistance to the attorney general in enforcing this chapter.

13-61-402. Enforcement powers of the attorney general.

(1) The attorney general has the exclusive authority to enforce this chapter.

(2) Upon referral from the division, the attorney general may initiate an enforcement action against a controller or processor for a violation of this chapter.

(3) (a) At least 30 days before the day on which the attorney general initiates an enforcement action against a controller or processor, the attorney general shall provide the controller or processor:

(i) written notice identifying each provision of this chapter the attorney general alleges the controller or processor has violated or is violating; and

(ii) an explanation of the basis for each allegation.

(b) The attorney general may not initiate an action if the controller or processor:

(i) cures the noticed violation within 30 days after the day on which the controller or processor receives the written notice described in Subsection (3)(a); and

(ii) provides the attorney general an express written statement that:

(A) the violation has been cured; and

(B) no further violation of the cured violation will occur.

(c) The attorney general may initiate an action against a controller or processor who:

(i) fails to cure a violation after receiving the notice described in Subsection (3)(a); or

(ii) after curing a noticed violation and providing a written statement in accordance with Subsection (3)(b), continues to violate this chapter.

(d) In an action described in Subsection (3)(c), the attorney general may recover:

(i) actual damages to the consumer; and

(ii) for each violation described in Subsection (3)(c), an amount not to exceed $7,500.

(4) All money received from an action under this chapter shall be deposited into the Consumer Privacy Account established in Section 13-61-403.

(5) If more than one controller or processor are involved in the same processing in violation of this chapter, the liability for the violation shall be allocated among the controllers or processors according to the principles of comparative fault.

13-61-403. Consumer Privacy Restricted Account.

(1) There is created a restricted account known as the "Consumer Privacy Account."

(2) The account shall be funded by money received through civil enforcement actions under this chapter.

(3) Upon appropriation, the division or the attorney general may use money deposited into the account for:

(a) investigation and administrative costs incurred by the division in investigating consumer complaints alleging violations of this chapter;

(b) recovery of costs and attorney fees accrued by the attorney general in enforcing this chapter; and

(c) providing consumer and business education regarding:

(i) consumer rights under this chapter; and

(ii) compliance with the provisions of this chapter for controllers and processors.

(4) If the balance in the account exceeds $4,000,000 at the close of any fiscal year, the Division of Finance shall transfer the amount that exceeds $4,000,000 into the General Fund.

13-61-404. Attorney general report.

(1) The attorney general and the division shall compile a report:

(a) evaluating the liability and enforcement provisions of this chapter, including the effectiveness of the attorney general's and the division's efforts to enforce this chapter; and

(b) summarizing the data protected and not protected by this chapter including, with reasonable detail, a list of the types of information that are publicly available from local, state, and federal government sources.

(2) The attorney general and the division may update the report as new information becomes available.

(3) The attorney general and the division shall submit the report to the Business and Labor Interim Committee before July 1, 2025.

Effective date.

This bill takes effect on December 31, 2023.

Virginia Consumer Data Protection Act

Chapter 53. Consumer Data Protection Act.

§ 59.1-575. Definitions.

As used in this chapter, unless the context requires a different meaning:

"Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity or shares common branding with another legal entity. For the purposes of this definition, "control" or "controlled" means (i) ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a company; (ii) control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or (iii) the power to exercise controlling influence over the management of a company.

"Authenticate" means verifying through reasonable means that the consumer, entitled to exercise his consumer rights in § 59.1-577, is the same consumer exercising such consumer rights with respect to the personal data at issue.

"Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. "Biometric data" does not include a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.

"Business associate" means the same meaning as the term established by HIPAA.

"Child" means any natural person younger than 13 years of age.

"Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. Consent may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action.

"Consumer" means a natural person who is a resident of the Commonwealth acting only in an individual or household context. It does not include a natural person acting in a commercial or employment context.

"Controller" means the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data.

"Covered entity" means the same as the term is established by HIPAA.

"Decisions that produce legal or similarly significant effects concerning a consumer" means a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.

"De-identified data" means data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person. A controller that possesses "de-identified data" shall comply with the requirements of subsection A of § 59.1-581.

"Health record" means the same as that term is defined in § 32.1-127.1:03.

"Health care provider" means the same as that term is defined in § 32.1-276.3.

"HIPAA" means the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d et seq.).

"Identified or identifiable natural person" means a person who can be readily identified, directly or indirectly.

"Institution of higher education" means a public institution and private institution of higher education, as those terms are defined in § 23.1-100.

"Nonprofit organization" means any corporation organized under the Virginia Nonstock Corporation Act (§ 13.1-801 et seq.) or any organization exempt from taxation under § 501(c)(3), 501(c)(6), or 501(c)(12) of the Internal Revenue Code, any political organization, any organization exempt from taxation under § 501(c)(4) of the Internal Revenue Code that is identified in § 52-41, and any subsidiary or affiliate of entities organized pursuant to Chapter 9.1 (§ 56-231.15 et seq.) of Title 56.

"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person.

"Personal data" does not include de-identified data or publicly available information.

"Political organization" means a party, committee, association, fund, or other organization, whether or not incorporated, organized and operated primarily for the purpose of influencing or attempting to influence the selection, nomination, election, or appointment of any individual to any federal, state, or local public office or office in a political organization or the election of a presidential/vice-presidential elector, whether or not such individual or elector is selected, nominated, elected, or appointed.

"Precise geolocation data" means information derived from technology, including but not limited to global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of a natural person with precision and accuracy within a radius of 1,750 feet. "Precise geolocation data" does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

"Process" or "processing" means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

"Processor" means a natural or legal entity that processes personal data on behalf of a controller.

"Profiling" means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

"Protected health information" means the same as the term is established by HIPAA.

"Pseudonymous data" means personal data that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

"Publicly available information" means information that is lawfully made available through federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.

"Sale of personal data" means the exchange of personal data for monetary consideration by the controller to a third party.

"Sale of personal data" does not include:

1. The disclosure of personal data to a processor that processes the personal data on behalf of the controller;
2. The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;
3. The disclosure or transfer of personal data to an affiliate of the controller;

4. The disclosure of information that the consumer (i) intentionally made available to the general public via a channel of mass media and (ii) did not restrict to a specific audience; or
5. The disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

"Sensitive data" means a category of personal data that includes:

1. Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;
2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;
3. The personal data collected from a known child; or
4. Precise geolocation data.

"State agency" means the same as that term is defined in § 2.2-307.

"Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests. "Targeted advertising" does not include:

1. Advertisements based on activities within a controller's own websites or online applications;
2. Advertisements based on the context of a consumer's current search query, visit to a website, or online application;
3. Advertisements directed to a consumer in response to the consumer's request for information or feedback; or
4. Processing personal data processed solely for measuring or reporting advertising performance, reach, or frequency.

"Third party" means a natural or legal person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller.

§ 59.1-576. Scope; exemptions.

A. This chapter applies to persons that conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth and that (i) during a calendar year, control or process personal data of at least 100,000 consumers or (ii) control or process personal data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data.

B.This chapter shall not apply to any (i) body, authority, board, bureau, commission, district, or agency of the Commonwealth or of any political subdivision of the Commonwealth; (ii) financial institution or data subject to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.); (iii) covered entity or business associate governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160 and 164 established pursuant to HIPAA, and the Health Information Technology for Economic and Clinical Health Act (P.L. 111-5); (iv) nonprofit organization; or (v) institution of higher education.

C. The following information and data is exempt from this chapter:

1. Protected health information under HIPAA;
2. Health records for purposes of Title 32.1;
3. Patient identifying information for purposes of 42 U.S.C. § 290dd-2;

4. Identifiable private information for purposes of the federal policy for the protection of human subjects under 45 C.F.R. Part 46; identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by The International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use; the protection of human subjects under 21 C.F.R. Parts 6, 50, and 56, or personal data used or shared in research conducted in accordance with the requirements set forth in this chapter, or other research conducted in accordance with applicable law;

5. Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986 (42 U.S.C. § 11101 et seq.);

6. Patient safety work product for purposes of the federal Patient Safety and Quality Improvement Act (42 U.S.C. § 299b-21 et seq.);

7. Information derived from any of the health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA;

8. Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as information exempt under this subsection that is maintained by a covered entity or business associate as defined by HIPAA or a program or a qualified service organization as defined by 42 U.S.C. § 290dd-2;

9. Information used only for public health activities and purposes as authorized by HIPAA;

10. The collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency or furnisher that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the federal Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.);

11. Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. § 2721 et seq.);

12. Personal data regulated by the federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g et seq.);

13. Personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act (12 U.S.C. § 2001 et seq.); and

14. Data processed or maintained (i) in the course of an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role; (ii) as the emergency contact information of an individual under this chapter used for emergency contact purposes; or (iii) that is necessary to retain to administer benefits for another individual relating to the individual under clause (i) and used for the purposes of administering those benefits.

D. Controllers and processors that comply with the verifiable parental consent requirements of the Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.) shall be deemed compliant with any obligation to obtain parental consent under this chapter.

§ 59.1-577. Personal data rights; consumers.

A. A consumer may invoke the consumer rights authorized pursuant to this subsection at any time by submitting a request to a controller specifying the consumer rights the consumer wishes to invoke. A known child's parent or legal guardian may invoke such consumer rights on behalf of the child regarding processing personal data belonging to the known child. A controller shall comply with an authenticated consumer request to exercise the right:

1. To confirm whether or not a controller is processing the consumer's personal data and to access such personal data;

2. To correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;

3. To delete personal data provided by or obtained about the consumer;

4. To obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means; and

5. To opt out of the processing of the personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

B. Except as otherwise provided in this chapter, a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to subsection A as follows:

1. A controller shall respond to the consumer without undue delay, but in all cases within 45 days of receipt of the request submitted pursuant to the methods described in subsection A. The response period may be extended once by 45 additional days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of any such extension within the initial 45-day response period, together with the reason for the extension.

2. If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but in all cases and at the latest within 45 days of receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision pursuant to subsection C.

3. Information provided in response to a consumer request shall be provided by a controller free of charge, up to twice annually per consumer. If requests from a consumer are manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of the request.

4. If a controller is unable to authenticate the request using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action under subsection A and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.

5. A controller that has obtained personal data about a consumer from a source other than the consumer shall be deemed in compliance with a consumer's request to delete such data pursuant to subdivision A 3 by either (i) retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the business's records and not using such retained data for any other purpose pursuant to the provisions of this chapter or (ii) opting the consumer out of the processing of such personal data for any purpose except for those exempted pursuant to the provisions of this chapter.

C. A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision pursuant to subdivision B 2. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to subsection A. Within 60 days of receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint.

§ 59.1-578. Data controller responsibilities; transparency.

A. A controller shall:

1. Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer;

2. Except as otherwise provided in this chapter, not process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;

3. Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue;

4. Not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer. However, nothing in this subdivision shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised his right to opt out pursuant to § 59.1-577 or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program; and

5. Not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with the federal Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.).

B. Any provision of a contract or agreement of any kind that purports to waive or limit in any way consumer rights pursuant to § 59.1-577 shall be deemed contrary to public policy and shall be void and unenforceable.

C. Controllers shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

1. The categories of personal data processed by the controller;

2. The purpose for processing personal data;

3. How consumers may exercise their consumer rights pursuant § 59.1-577, including how a consumer may appeal a controller's decision with regard to the consumer's request;

4. The categories of personal data that the controller shares with third parties, if any; and

5. The categories of third parties, if any, with whom the controller shares personal data.

D. If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing.

E. A controller shall establish, and shall describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights under this chapter. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests, and the ability of the controller to authenticate the identity of the consumer making the request. Controllers shall not require a consumer to create a new account in order to exercise consumer rights pursuant to § 59.1-577 but may require a consumer to use an existing account.

§ 59.1-579. Responsibility according to role; controller and processor.

A. A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under this chapter. Such assistance shall include:

1. Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as this is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests pursuant to § 59.1-577.

2. Taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security of the system of the processor pursuant to § 18.2-186.6 in order to meet the controller's obligations.

3. Providing necessary information to enable the controller to conduct and document data protection assessments pursuant to § 59.1-580.

B. A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract shall also include requirements that the processor shall:

1. Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

2. At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

3. Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this chapter;

4. Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this chapter using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request; and

5. Engage any subcontractor pursuant to a written contract in accordance with subsection C that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

C. Nothing in this section shall be construed to relieve a controller or a processor from the liabilities imposed on it by virtue of its role in the processing relationship as defined by this chapter.

D. Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor.

§ 59.1-580. Data protection assessments.

A. A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data:

1. The processing of personal data for purposes of targeted advertising;

2. The sale of personal data;

3.The processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial, physical, or reputational injury to consumers; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers;

4. The processing of sensitive data; and

5. Any processing activities involving personal data that present a heightened risk of harm to consumers.

B. Data protection assessments conducted pursuant to subsection A shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, shall be factored into this assessment by the controller.

C. The Attorney General may request, pursuant to a civil investigative demand, that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in § 59.1-578. Data protection assessments shall be confidential and exempt from public inspection and copying under the Virginia Freedom of Information Act (§ 2.2-3700 et seq.). The disclosure of a data protection assessment pursuant to a request from the Attorney General shall not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

D. A single data protection assessment may address a comparable set of processing operations that include similar activities.

E. Data protection assessments conducted by a controller for the purpose of compliance with other laws or regulations may comply under this section if the assessments have a reasonably comparable scope and effect.

F. Data protection assessment requirements shall apply to processing activities created or generated after January 1, 2023, and are not retroactive.

§ 59.1-581. Processing de-identified data; exemptions.

A. The controller in possession of de-identified data shall:

1. Take reasonable measures to ensure that the data cannot be associated with a natural person;

2. Publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and

3. Contractually obligate any recipients of the de-identified data to comply with all provisions of this chapter.

B. Nothing in this chapter shall be construed to (i) require a controller or processor to re-identify de-identified data or pseudonymous data or (ii) maintain data in identifiable form, or collect, obtain, retain, or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data.

C. Nothing in this chapter shall be construed to require a controller or processor to comply with an authenticated consumer rights request, pursuant to § 59.1-577, if all of the following are true:

1. The controller is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data;

2. The controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer; and

3. The controller does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.

D. The consumer rights contained in subdivisions A 1 through 4 of § 59.1-577 and § 59.1-578 shall not apply to pseudonymous data in cases where the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.

E. A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

§ 59.1-582. Limitations.

A. Nothing in this chapter shall be construed to restrict a controller's or processor's ability to:

1. Comply with federal, state, or local laws, rules, or regulations;

2. Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

3. Cooperate with law-enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;

4. Investigate, establish, exercise, prepare for, or defend legal claims;

5. Provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer prior to entering into a contract;

6. Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis;

7. Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action;

8. Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, or similar independent oversight entities that determine: (i) if the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller; (ii) the expected benefits of the research outweigh the privacy risks; and (iii) if the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification; or

9. Assist another controller, processor, or third party with any of the obligations under this subsection.

B. The obligations imposed on controllers or processors under this chapter shall not restrict a controller's or processor's ability to collect, use, or retain data to:

1. Conduct internal research to develop, improve, or repair products, services, or technology;

2. Effectuate a product recall;

3. Identify and repair technical errors that impair existing or intended functionality; or

4. Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

C. The obligations imposed on controllers or processors under this chapter shall not apply where compliance by the controller or processor with this chapter would violate an evidentiary privilege under the laws of the Commonwealth. Nothing in this chapter shall be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of the Commonwealth as part of a privileged communication.

D. A controller or processor that discloses personal data to a third-party controller or processor, in compliance with the requirements of this chapter, is not in violation of this chapter if the third-party controller or processor that receives and processes such personal data is in violation of this chapter, provided that, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation. A third-party controller or processor receiving personal data from a controller or processor in compliance with the requirements of this chapter is likewise not in violation of this chapter for the transgressions of the controller or processor from which it receives such personal data.

E. Nothing in this chapter shall be construed as an obligation imposed on controllers and processors that adversely affects the rights or freedoms of any persons, such as exercising the right of free speech pursuant to the First Amendment to the United States Constitution, or applies to the processing of personal data by a person in the course of a purely personal or household activity.

F. Personal data processed by a controller pursuant to this section shall not be processed for any purpose other than those expressly listed in this section unless otherwise allowed by this chapter. Personal data processed by a controller pursuant to this section may be processed to the extent that such processing is:

1. Reasonably necessary and proportionate to the purposes listed in this section; and

2. Adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section. Personal data collected, used, or retained pursuant to subsection B shall, where applicable, take into account the nature and purpose or purposes of such collection, use, or retention. Such data shall be subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to such collection, use, or retention of personal data.

G. If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in subsection F.

H. Processing personal data for the purposes expressly identified in subdivisions A 1 through 9 shall not solely make an entity a controller with respect to such processing.

§ 59.1-583. Investigative authority.

Whenever the Attorney General has reasonable cause to believe that any person has engaged in, is engaging in, or is about to engage in any violation of this chapter, the Attorney General is empowered to issue a civil investigative demand. The provisions of § 59.1-9.10 shall apply mutatis mutandis to civil investigative demands issued under this section.
2021, Sp. Sess. I, cc. 35, 36.

§ 59.1-584. Enforcement; civil penalty; expenses.

A. The Attorney General shall have exclusive authority to enforce the provisions of this chapter.

B. Prior to initiating any action under this chapter, the Attorney General shall provide a controller or processor 30 days' written notice identifying the specific provisions of this chapter the Attorney General alleges have been or are being violated. If within the 30-day period the controller or processor cures the noticed violation and provides the Attorney General an express written statement that the alleged violations have been cured and that no further violations shall occur, no action shall be initiated against the controller or processor.

C. If a controller or processor continues to violate this chapter following the cure period in subsection B or breaches an express written statement provided to the Attorney General under that subsection, the Attorney General may initiate an action in the name of the Commonwealth and may seek an injunction to restrain any violations of this chapter and civil penalties of up to $7,500 for each violation under this chapter. All civil penalties, expenses, and attorney fees collected pursuant to this chapter shall be paid into the state treasury and credited to the Regulatory, Consumer Advocacy, Litigation, and Enforcement Revolving Trust Fund.

D. The Attorney General may recover reasonable expenses incurred in investigating and preparing the case, including attorney fees, in any action initiated under this chapter.

E. Nothing in this chapter shall be construed as providing the basis for, or be subject to, a private right of action for violations of this chapter or under any other law.

§ 59.1-585. Repealed.

Repealed by Acts 2022, cc. 451 and 452, cl. 2.

EU General Data Protection Regulation

CHAPTER I GENERAL PROVISIONS

Article 1 Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Article 2 Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

   (a) in the course of an activity which falls outside the scope of Union law;

   (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

   (c) by a natural person in the course of a purely personal or household activity;

   (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.

4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Article 3 Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

   (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Article 4 Definitions

For the purposes of this Regulation:

1. 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

2. 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

3. 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

4. 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

5. 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

6. 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

7. 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

8. 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

9. 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

10 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

11. ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

12. ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

13. ‘genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

14. ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

15. ‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

16. ‘main establishment’ means:

    (a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

    (b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

17 ‘representative’ means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

18. ‘enterprise’ means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

19. ‘group of undertakings’ means a controlling undertaking and its controlled undertakings;

20 ‘binding corporate rules’ means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

21. ‘supervisory authority’ means an independent public authority which is established by a Member State pursuant to Article 51;

22. ‘supervisory authority concerned’ means a supervisory authority which is concerned by the processing of personal data because:

    (a) the controller or processor is established on the territory of the Member State of that supervisory authority;

(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

(c) a complaint has been lodged with that supervisory authority;

23. 'cross-border processing' means either:

(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

24. 'relevant and reasoned objection' means an objection as to whether there is an infringement of this Regulation or not, or whether the envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

25. 'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council[1];

26. 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

CHAPTER II PRINCIPLES

Article 5 Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

[1] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 6 Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data

which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

   (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

   (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

   (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

   (d) the possible consequences of the intended further processing for data subjects;

   (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 7 Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw consent as to give it.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 8 Conditions applicable to child's consent in relation to information society services

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

   Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

Article 9 Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; or

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Article 10 Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Article 11 Processing which does not require identification

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

CHAPTER III RIGHTS OF THE DATA SUBJECT

Section 1 Transparency and Modalities

Article 12 Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

   (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

   (b) refuse to act on the request.

   The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

Section 2 Information and Access to Personal Data

Article 13 Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

   (a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

   (b) the contact details of the data protection officer, where applicable;

   (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

   (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point
(a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Article 14 Information to be provided where personal data have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller and, if any, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, where applicable;

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(e) the right to lodge a complaint with a supervisory authority;

(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

(g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Article 15 Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information:

   (a) the purposes of the processing;

   (b) the categories of personal data concerned;

   (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

   (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

   (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

   (f) the right to lodge a complaint with a supervisory authority;

   (g) where the personal data are not collected from the data subject, any available information as to their source;

   (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Section 3 Rectification and Erasure

Article 16 Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her . Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Article 17 Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

   (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

   (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

   (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

   (d) the personal data have been unlawfully processed;

   (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

   (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

   (a) for exercising the right of freedom of expression and information;

   (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

   (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

   (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

   (e) for the establishment, exercise or defence of legal claims.

Article 18 Right to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

   (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

   (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

   (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

   (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Article 19 Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Articles 16, 17(1) and 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 20 Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

   (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

   (b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Article 21 Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on points (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Article 22 Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

   (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

   (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

   (c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) apply and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Article 23 Restrictions

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

   (a) national security;

   (b) defence;

   (c) public security;

   (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

   (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;

   (f) the protection of judicial independence and judicial proceedings;

   (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

   (h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a), (b), (c), (d), (e) and (g);

   (i) the protection of the data subject or the rights and freedoms of others;

   (j) the enforcement of civil law claims.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

   (a) the purposes of the processing or categories of processing;

   (b) the categories of personal data;

   (c) the scope of the restrictions introduced;

   (d) the safeguards to prevent abuse or unlawful access or transfer;

   (e) the specification of the controller or categories of controllers;

   (f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

   (g) the risks to the rights and freedoms of data subjects; and

   (h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

CHAPTER IV CONTROLLER AND PROCESSOR

Section 1 General Obligations

Article 24 Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Article 25 Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Article 26 Joint controllers

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Article 27 Representatives of controllers or processors not established in the Union

1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

2. This obligation shall not apply to:

   (a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

   (b) a public authority or body.

3. The representative shall be established in one of those Member States where the data subjects are and whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored.

4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Article 28 Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

   (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

   (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

   (c) takes all measures required pursuant to Article 32;

   (d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 29 Processing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Article 30 Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

   (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

   (b) the purposes of the processing;

   (c) a description of the categories of data subjects and of the categories of personal data;

   (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

   (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of appropriate safeguards;

   (f) where possible, the envisaged time limits for erasure of the different categories of data;

   (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

   (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

   (b) the categories of processing carried out on behalf of each controller;

   (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of appropriate safeguards;

   (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

Article 31 Cooperation with the supervisory authority

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

Article 32 Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

   (a) the pseudonymisation and encryption of personal data;

   (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

   (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 33 Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

   (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

   (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

   (c) describe the likely consequences of the personal data breach;

   (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5 The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Section 3 Data Protection Impact Assessment and Prior Consultation

Article 34 Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

   (a) the controller has implemented appropriate technical and organisational protection measures, and that those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

   (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

   (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Article 35 Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

   (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Article 36 Prior consultation

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

   (a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

   (b) the purposes and means of the intended processing;

   (c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

   (d) where applicable, the contact details of the data protection officer;

   (e) the data protection impact assessment provided for in Article 35; and

   (f) any other information requested by the supervisory authority.

4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

Section 4 Data Protection Officer

Article 37 Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

   (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

   (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

   (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

Article 38 Position of the data protection officer

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Article 39 Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks:

   (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

   (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness- raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Section 5 Codes of Conduct and Certification

Article 40 Codes of conduct

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:

(a) fair and transparent processing;

(b) the legitimate interests pursued by controllers in specific contexts;

(c) the collection of personal data;

(d) the pseudonymisation of personal data;

(e) the information provided to the public and to data subjects;

(f) the exercise of the rights of data subjects;

(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

(h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;

(i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;

(j) the transfer of personal data to third countries or international organisations; or

(k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

3. In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate

safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

4. A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.

5. Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

6. Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.

7. Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3, provides appropriate safeguards.

8. Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.

9. The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

10. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9.

11. The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

Article 41 Monitoring of approved codes of conduct

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

(a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

(b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

(c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(d) demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The competent supervisory authority shall submit the draft requirements for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.

4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5. The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the requirements for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.

6. This Article shall not apply to processing carried out by public authorities and bodies.

Article 42 Certification

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

3. The certification shall be voluntary and available via a process that is transparent.

4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant criteria continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the criteria for the certification are not or are no longer met.

8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

Article 43 Certification bodies

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:

   (a) the supervisory authority which is competent pursuant to Article 55 or 56;

   (b) the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council[2] in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.

2. Certification bodies referred to in paragraph 1 shall be accredited in accordance with paragraph 1 only where they have:

   (a) demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;

   (b) undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;

   (c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;

   (d) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

   (e) demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.

3. The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of requirements approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

[2] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

4. The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

5. The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.

6. The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board.

7. Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).

9. The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

CHAPTER V TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Article 44 General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Article 45 Transfers on the basis of an adequacy decision

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

   (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro- active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

6. On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

7. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

8. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.

9. The Commission shall publish in the *Official Journal of the European Union* and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

10. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

Article 46 Transfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

   (a) a legally binding and enforceable instrument between public authorities or bodies;

   (b) binding corporate rules in accordance with Article 47;

   (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

   (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

   (e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

   (f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

   (a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

   (b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.

5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/ EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

Article 47 Binding corporate rules

1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

   (a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

   (b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

   (c) fulfill the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

   (a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

   (b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

   (c) their legally binding nature, both internally and externally;

   (d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

   (e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

   (f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

   (g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;

   (h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint- handling;

   (i) the complaint procedures;

   (j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred under point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

(k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

(l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

(m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(n) the appropriate data protection training to personnel having permanent or regular access to personal data.

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

Article 48 Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 49 Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre- contractual measures taken at the data subject's request;

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Articles 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation pursuant to points (a) to (g) of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph and the second subparagraph of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

Article 50 International cooperation for the protection of personal data

In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

CHAPTER VI INDEPENDENT SUPERVISORY AUTHORITIES

Section 1 Independent Status

Article 51 Supervisory authority

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union.

2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.

4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by … [*two years from the date of entry into force of this Regulation*] at the latest and, without delay, any subsequent amendment affecting them.

Article 52 Independence

1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.

2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

Article 53 General conditions for the members of the supervisory authority

1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:

   — their parliament;

   — their government;

   — their head of State; or

   — an independent body entrusted with the appointment under Member State law.

2. Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.

3 The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.

4. A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

Article 54 Rules on the establishment of the supervisory authority

1. Each Member State shall provide by law for all of the following:

   (a) the establishment of each supervisory authority;

   (b) the qualifications and eligibility conditions required to be appointed as member of each supervisory authority;

   (c) the rules and procedures for the appointment of the member or members of each supervisory authority;

   (d) the duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after … [*the date of entry into force of this Regulation*], part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;

   (e) whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;

   (f) the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Regulation.

Article 55 Competence

1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

2. Where processing is carried out by public authorities or private bodies acting on the basis of points (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

Article 56 Competence of the lead supervisory authority

1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).

5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.

6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

Article 57 Tasks

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

   (a) monitor and enforce the application of this Regulation;

   (b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

   (c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(d) promote the awareness of controllers and processors of their obligations under this Regulation;

(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

(i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(j) adopt standard contractual clauses referred to in Article 28(8) and point (d) of Article 46(2);

(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);

(l) give advice on the processing operations referred to in Article 36(2);

(m) encourage the drawing up of codes of conduct pursuant to Article 40 and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);

(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);

(o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);

(p) draft and publish the requirements for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(r) authorise contractual clauses and provisions referred to in Article 46(3);

(s) approve binding corporate rules pursuant to Article 47;

(t) contribute to the activities of the Board;

(u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and

(v) fulfill any other tasks related to the protection of personal data.

2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1, by measures such as a complaint submission form which may also be completed electronically, without excluding other means of communication.

3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer.

4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 58 Powers

1. Each supervisory authority shall have all of the following investigative powers:

   (a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

   (b) to carry out investigations in the form of data protection audits;

   (c) to carry out a review on certifications issued pursuant to Article 42(7);

   (d) to notify the controller or the processor of an alleged infringement of this Regulation;

   (e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

   (f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

2. Each supervisory authority shall have all of the following corrective powers:

   (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

   (b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

   (c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

   (d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

   (e) to order the controller to communicate a personal data breach to the data subject;

   (f) to impose a temporary or definitive limitation including a ban on processing;

   (g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Articles 17(2) and 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

3. Each supervisory authority shall have all of the following authorisation and advisory powers:

(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;

(b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

(c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;

(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);

(e) to accredit certification bodies pursuant to Article 43;

(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);

(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(h) to authorise contractual clauses referred to in point (a) of Article 46(3);

(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);

(j) to approve binding corporate rules pursuant to Article 47.

4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.

5. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.

6. Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII.

Article 59 Activity reports

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

CHAPTER VII COOPERATION AND CONSISTENCY

Section 1 Cooperation

Article 60 Cooperation between the lead supervisory authority and other supervisory authorities concerned

1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.

2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.

3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.

4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion it is not relevant and reasoned, submit the matter to the consistency mechanism referred to in Article 63.

5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.

6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.

7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.

8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

9. Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.

10. After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.

11. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.

12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.

Article 61 Mutual assistance

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

2. Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

3. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

4. The requested supervisory authority shall not refuse to comply with the request unless:

   (a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or

   (b) compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.

5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.

6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.

7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

8. Where a supervisory authority does not provide the information referred to in paragraph 5 within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).

9. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Article 62 Joint operations of supervisory authorities

1. The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff from the supervisory authorities of other Member States are involved.

2. Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. The supervisory authority which is competent pursuant to Article 56 (1) or 56(4) shall invite the supervisory authority of each of those Member States to take part in the joint operations and shall respond without delay to the request of a supervisory authority to participate.

3. A supervisory authority may, in accordance with Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the Member State law of the host supervisory authority.

4. Where, in accordance with paragraph 1, staff of a seconding supervisory authority operate in another Member State, the Member State of the host supervisory authority shall assume responsibility for their actions, including liability, for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.

5. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse that other Member State in full any sums it has paid to the persons entitled on their behalf.

6. Without prejudice to the exercise of its rights vis-à-vis third parties and with the exception of paragraph 5, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement from another Member State in relation to damage referred to in paragraph 4.

7. Where a joint operation is intended and a supervisory authority does not, within one month, comply with the obligation laid down in the second sentence of paragraph 2 of this Article, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 55. In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an opinion or an urgent binding decision from the Board pursuant to Article 66(2).

Section 2 Consistency

Article 63 Consistency mechanism

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.

Article 64 Opinion of the Board

1. The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it:

   (a) aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4);

   (b) concerns a matter pursuant to Article 40(7) whether a draft code of conduct or an amendment or extension to a code of conduct complies with this Regulation;

   (c) aims to approve the requirements for accreditation of a body pursuant to Article 41(3), of a certification body pursuant to Article 43(3) or the criteria for certification referred to in Article 42(5);

   (d) aims to determine standard data protection clauses referred to in point (d) of Article 46(2) and Article 28(8);

   (e) aims to authorise contractual clauses referred to in point (a) of Article 46(3); or

   (f) aims to approve binding corporate rules within the meaning of Article 47.

2. Any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.

3. In the cases referred to in paragraphs 1 and 2, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be adopted within eight weeks by simple majority of the members of the Board. That period may be extended by a further six weeks, taking into account the complexity of the subject matter. Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 5, a member which has not objected within a reasonable period indicated by the Chair, shall be deemed to be in agreement with the draft decision.

4. Supervisory authorities and the Commission shall, without undue delay, communicate by electronic means to the Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft decision, the grounds which make the enactment of such measure necessary, and the views of other supervisory authorities concerned.

5. The Chair of the Board shall, without undue, delay inform by electronic means:

   (a) the members of the Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat of the Board shall, where necessary, provide translations of relevant information; and

   (b) the supervisory authority referred to, as the case may be, in paragraphs 1 and 2, and the Commission of the opinion and make it public.

6. The competent supervisory authority referred to in paragraph 1 shall not adopt its draft decision referred to in paragraph 1 within the period referred to in paragraph 3.

7. The competent supervisory authority referred to in paragraph 1 shall take utmost account of the opinion of the Board and shall, within two weeks after receiving the opinion, communicate to the Chair of the Board by electronic means whether it will maintain or amend its draft decision and, if any, the amended draft decision, using a standardised format.

8. Where the competent supervisory authority referred to in paragraph1 informs the Chair of the Board within the period referred to in paragraph 7 of this Article that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, Article 65(1) shall apply.

Article 65 Dispute resolution by the Board

1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:

   (a) where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead supervisory authority and the lead supervisory authority has not followed the objection or has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;

   (b) where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;

   (c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.

2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-third majority of the members of the Board. This period may be extended by a further month on account of the complexity of the subject-matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.

3. Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where the members of the Board are split, the decision shall by adopted by the vote of its Chair.

4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.

5. The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. It shall inform the Commission thereof. The decision shall be published on the website of the Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.

6. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this Article and shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.

Article 66 Urgency procedure

1. In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.

2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision.

3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.

4. By derogation from Articles 64(3) and 65(2), an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the Board.

Section 3 European Data Protection Board

Article 67 Exchange of information

The Commission may adopt implementing acts of general scope in order to specify the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in Article 64.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Article 68 European Data Protection Board

1. The European Data Protection Board (the 'Board') is hereby established as a body of the Union and shall have legal personality.

2. The Board shall be represented by its Chair.

3. The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.

4. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance with that Member State's law.

5. The Commission shall have the right to participate in the activities and meetings of the Board without voting right. The Commission shall designate a representative. The Chair of the Board shall communicate to the Commission the activities of the Board.

6. In the cases referred to in Article 65, the European Data Protection Supervisor shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation.

Article 69 Independence

1. The Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 70 and 71.

2. Without prejudice to requests by the Commission referred to in Article 70(1) and (2), the Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.

Article 70 Tasks of the Board

1. The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular:

   (a) monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 without prejudice to the tasks of national supervisory authorities;

   (b) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;

   (c) advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules;

   (d) issue guidelines, recommendations, and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services as referred to in Article 17 (2);

   (e) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation;

   (f) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(2);

   (g) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing the personal data breaches and determining the undue delay referred to in Article 33(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;

   (h) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons referred to in Article 34(1).

   (I) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for personal data transfers based on binding corporate rules adhered to by controllers and binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned referred to in Article 47;

   (j) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for the personal data transfers on the basis of Article 49(1);

   (k) draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 58(1), (2) and (3) and the fixing of administrative fines pursuant to Articles 83;

   (l) review the practical application of the guidelines, recommendations and best practices;

(m) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing common procedures for reporting by natural persons of infringements of this Regulation pursuant to Article 54(2);

(n) encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 40 and 42;

(o) approve the criteria of certification pursuant to Article 42(5) and maintain a public register of certification mechanisms and data protection seals and marks pursuant to Article 42(8) and of the certified controllers or processors established in third countries pursuant to Article 42(7);

(p) approve the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies referred to in Article 43;

(q) provide the Commission with an opinion on the certification requirements referred to in Article 43(8);

(r) provide the Commission with an opinion on the icons referred to in Article 12(7);

(s) provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country or international organisation, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organisation no longer ensures an adequate level of protection. To that end, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organisation.

(t) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant to Article 64(2) and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66;

(u) promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;

(v) promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations;

(w) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.

(x) issue opinions on codes of conduct drawn up at Union level pursuant to Article 40(9); and

(y) maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.

2. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 93 and make them public.

4. The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The Board shall, without prejudice to Article 76, make the results of the consultation procedure publicly available.

Article 71 Reports

1. The Board shall draw up an annual report regarding the protection of natural persons with regard to processing in the Union and, where relevant, in third countries and international organisations. The report shall be made public and be transmitted to the European Parliament, to the Council and to the Commission.

2. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (l) of Article 70(1) as well as of the binding decisions referred to in Article 65.

Article 72 Procedure

1. The Board shall take decisions by a simple majority of its members, unless otherwise provided for in this Regulation.

2. The Board shall adopt its own rules of procedure by a two-third majority of its members and organise its own operational arrangements.

Article 73 Chair

1. The Board shall elect a chair and two deputy chairs from amongst its members by simple majority.

2. The term of office of the Chair and of the deputy chairs shall be five years and be renewable once.

Article 74 Tasks of the Chair

1. The Chair shall have the following tasks:

   (a) to convene the meetings of the Board and prepare its agenda;

   (b) to notify decisions adopted by the Board pursuant to Article 65 to the lead supervisory authority and the supervisory authorities concerned;

   (c) to ensure the timely performance of the tasks of the Board, in particular in relation to the consistency mechanism referred to in Article 63.

2. The Board shall lay down the allocation of tasks between the Chair and the deputy chairs in its rules of procedure.

Article 75 Secretariat

1. The Board shall have a secretariat, which shall be provided by the European Data Protection Supervisor.

2. The secretariat shall perform its tasks exclusively under the instructions of the Chair of the Board.

3. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation shall be subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor.

4. Where appropriate, the Board and the European Data Protection Supervisor shall establish and publish a Memorandum of Understanding implementing this Article, determining the terms of their cooperation, and applicable to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation.

5. The secretariat shall provide analytical, administrative and logistical support to the Board.

6. The secretariat shall be responsible in particular for:

(a) the day-to-day business of the Board;

(b) communication between the members of the Board, its Chair and the Commission;

(c) communication with other institutions and the public;

(d) the use of electronic means for the internal and external communication;

(e) the translation of relevant information;

(f) the preparation and follow-up of the meetings of the Board;

(g) the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the Board.

Article 76 Confidentiality

1. The discussions of the Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure.

2. Access to documents submitted to members of the Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001 of the European Parliament and of the Council[3].

CHAPTER VIII REMEDIES, LIABILITY AND PENALTIES

Article 77 Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

Article 78 Right to an effective judicial remedy against a supervisory authority

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

[3] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Article 55 and Article 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.

3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

4. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

Article 79 Right to an effective judicial remedy against a controller or processor

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

Article 80 Representation of data subjects

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

Article 81 Suspension of proceedings

1. Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.

2. Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.

3. Where those proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.

Article 82 Right to compensation and liability

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

Article 83 General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

   (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

   (b) the intentional or negligent character of the infringement;

   (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

   (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

   (e) any relevant previous infringements by the controller or processor;

   (f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

   (g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) in case measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 and 43;

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(d) any obligations pursuant to Member State law adopted under Chapter IX;

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by … [*two years from the date of entry into force of this Regulation*] and, without delay, any subsequent amendment law or amendment affecting them.

Article 84 Penalties

1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by … [*two years from the date of entry into force of this Regulation*] and, without delay, any subsequent amendment affecting them.

CHAPTER IX PROVISIONS RELATING TO SPECIFIC PROCESSING SITUATIONS

Article 85 Processing and freedom of expression and information

1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

Article 86 Processing and public access to official documents

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

Article 87 Processing of the national identification number

Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

Article 88 Processing in the context of employment

1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by … [*two years from the date of entry into force of this Regulation*] and, without delay, any subsequent amendment affecting them.

Article 89 Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

Article 90 Obligations of secrecy

1. Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.

2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by … [*two years from the date of entry into force of this Regulation*] and, without delay, any subsequent amendment affecting them.

Article 91 Existing data protection rules of churches and religious associations

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules may continue to apply, provided that they are brought into line with this Regulation.

2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 shall be subject to the supervision of an independent supervisory authority, which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.

CHAPTER X DELEGATED ACTS AND IMPLEMENTING ACTS

Article 92 Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The delegation of power referred to in Article 12(8) and Article 43(8) shall be conferred on the Commission for an indeterminate period of time from … [*the date of entry into force of this Regulation*].

3. The delegation of power referred to in Article 12(8) and Article 43(8) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 12(8) and Article 43(8) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Article 93 Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

CHAPTER XI FINAL PROVISIONS

Article 94 Repeal of Directive 95/46/EC

1. Directive 95/46/EC is repealed with effect from … [*two years from the date of entry into force of this Regulation*].

2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

Article 95 Relationship with Directive 2002/58/EC

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

Article 96 Relationship with previously concluded Agreements

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to … [*the date of entry into force of this Regulation*], and which are in accordance with Union law applicable prior to … [*the date of entry into force of this Regulation*], shall remain in force until amended, replaced or revoked.

Article 97 Commission reports

1. By … [*4 years after the date of entry into force of this Regulation*] and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.

2. In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of:

   (a) Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC;

   (b) Chapter VII on cooperation and consistency.

3. For the purpose of paragraph 1, the Commission may request information from Member States and supervisory authorities.

4. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources.

5. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account of developments in information technology and in the light of the state of progress in the information society.

Article 98 Review of other Union legal acts on data protection

The Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. This shall in particular concern the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data.

Article 99 Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. It shall apply from … [*two years from the date of entry into force of this Regulation*].

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Recitals (EU General Data Protection Regulation)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments, Having regard to the opinion of the European Economic and Social Committee[1], Having regard to the opinion of the Committee of the Regions[2],

Acting in accordance with the ordinary legislative procedure[3], Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

(3) Directive 95/46/EC of the European Parliament and of the Council (4) seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

(4) The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

(5) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased. National authorities in the Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.

(6) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.

---

[1] OJ C 229, 31.7.2012, p. 90.
[2] OJ C 391, 18.12.2012, p. 127.
[3] Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.

(7) Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.

(8) Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law.

(9) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.

(10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data'). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.

(11) Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.

(12) Article 16(2) TFEU mandates the European Parliament and the Council to lay down the rules relating to the protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of personal data.

(13) In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the

Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC[4].

(14) The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

(15) In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

(16) This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.

(17) Regulation (EC) No 45/2001 of the European Parliament and of the Council[5] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data should be adapted to the principles and rules established in this Regulation and applied in the light of this Regulation. In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Regulation (EC) No 45/2001 should follow after the adoption of this Regulation, in order to allow application at the same time as this Regulation.

(18) This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.

(19) The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council[6]. Member States may entrust competent authorities within the meaning of Directive (EU) 2016/680 with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or

---

[4] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C(2003) 1422) (OJ L 124, 20.5.2003, p. 36).

[5] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

[6] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA (see page 89 of this Official Journal).

prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of this Regulation.

With regard to the processing of personal data by those competent authorities for purposes falling within scope of this Regulation, Member States should be able to maintain or introduce more specific provisions to adapt the application of the rules of this Regulation. Such provisions may determine more precisely specific requirements for the processing of personal data by those competent authorities for those other purposes, taking into account the constitutional, organisational and administrative structure of the respective Member State. When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.

(20) While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.

(21) This Regulation is without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council[7], in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States.

(22) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

(23) In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

[7] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

(24) The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

(25) Where Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.

(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

(27) This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.

(28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

(29) In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller.

(30) Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

(31) Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing.

(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

(33) It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

(34) Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

(35) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council[8] to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

(36) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered

[8] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

(37) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings.

(38) Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

(39) Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

(40) In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

(41) Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights.

(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given.

In accordance with Council Directive 93/13/EEC[9] a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

(43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

(44) Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract.

(45) Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.

(46) The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

(47) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in

[9] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29).

particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

(48) Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.

(49) The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

(50) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected.

In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

(51) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

(52) Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health- care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

(53) Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.

(54) The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council[10], namely all elements related to health,

[10] Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70).

namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

(55) Moreover, the processing of personal data by official authorities for the purpose of achieving the aims, laid down by constitutional law or by international public law, of officially recognised religious associations, is carried out on grounds of public interest.

(56) Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.

(57) If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.

(58) The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

(59) Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

(60) The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.

(61) The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected,

the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.

(62) However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.

(63) A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

(64) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

(65) A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

(66) To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.

(67) Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.

(68) To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.

(69) Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.

(70) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.

(71) The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.

In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject, and prevent, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or processing that results in measures having such an effect.

(72) Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles. The European Data Protection Board established by this Regulation (the 'Board') should be able to issue guidance in that context.

(73) Restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling, as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for regulated professions, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes. Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(74) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

(75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

(76) The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

(77) Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.

(78) The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

(79) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(80) Where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union whose processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or to the monitoring of their behaviour as far as their behaviour takes place within the Union, the controller or the processor should designate a representative, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing or if the controller is a public authority or body. The representative should act on behalf of the controller or the processor and may be addressed by any supervisory authority. The representative should be explicitly designated by a written mandate of the controller or of the processor to act on its behalf with regard to its obligations under this Regulation. The designation of such a representative does not affect the responsibility or liability of the controller or of the processor under this Regulation. Such a representative should perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation. The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.

(81) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific

tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject.

(82) In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.

(83) In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

(84) In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

(85) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

(86) The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

(87) It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

(88) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.

(89) Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.

(90) In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.

(91) This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.

(92) There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

(93) In the context of the adoption of the Member State law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question, Member States may deem it necessary to carry out such assessment prior to the processing activities.

(94) Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.

(95) The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

(96) A consultation of the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data, in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.

(97) Where the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity, where, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. In the private sector, the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities. The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor. Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

(98) Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons.

(99) When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations.

(100) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.

(101) Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.

(102) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.

(103) The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision.

(104) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

(105) Apart from the international commitments the third country or international organisation has entered into, the Commission should take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult the Board when assessing the level of protection in third countries or international organisations.

(106) The Commission should monitor the functioning of decisions on the level of protection in a third country, a territory or specified sector within a third country, or an international organisation, and monitor the functioning of decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC. In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning. That periodic review should be conducted in consultation with the third country or international organisation in question and take into account all relevant developments in the

third country or international organisation. For the purposes of monitoring and of carrying out the periodic reviews, the Commission should take into consideration the views and findings of the European Parliament and of the Council as well as of other relevant bodies and sources. The Commission should evaluate, within a reasonable time, the functioning of the latter decisions and report any relevant findings to the Committee within the meaning of Regulation (EU) No 182/2011 of the European Parliament and of the Council[11] as established under this Regulation, to the European Parliament and to the Council.

(107) The Commission may recognise that a third country, a territory or a specified sector within a third country, or an international organisation no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers subject to appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

(108) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding.

(109) The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.

(110) A group of undertakings, or a group of enterprises engaged in a joint economic activity, should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same group of undertakings, or group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

(111) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including

[11] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In the latter case, such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.

(112) Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organisation. Member States should notify such provisions to the Commission. Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject.

(113) Transfers which can be qualified as not repetitive and that only concern a limited number of data subjects, could also be possible for the purposes of the compelling legitimate interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer. The controller should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data. Such transfers should be possible only in residual cases where none of the other grounds for transfer are applicable. For scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. The controller should inform the supervisory authority and the data subject about the transfer.

(114) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.

(115) Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject.

(116) When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information.

At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international cooperation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in accordance with this Regulation.

(117) The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States should be able to establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.

(118) The independence of supervisory authorities should not mean that the supervisory authorities cannot be subject to control or monitoring mechanisms regarding their financial expenditure or to judicial review.

(119) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth cooperation with other supervisory authorities, the Board and the Commission.

(120) Each supervisory authority should be provided with the financial and human resources, premises and infrastructure necessary for the effective performance of their tasks, including those related to mutual assistance and cooperation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget.

(121) The general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members are to be appointed, by means of a transparent procedure, either by the parliament, government or the head of State of the Member State on the basis of a proposal from the government, a member of the government, the parliament or a chamber of the parliament, or by an independent body entrusted under Member State law. In order to ensure the independence of the supervisory authority, the member or members should act with integrity, refrain from any action that is incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not. The supervisory authority should have its own staff, chosen by the supervisory authority or an independent body established by Member State law, which should be subject to the exclusive direction of the member or members of the supervisory authority.

(122) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should cover in particular the processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State, the processing of personal data carried out by public authorities or private bodies acting in the public interest, processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the Union when targeting data subjects residing on its territory. This should include handling complaints lodged by a data subject, conducting investigations on the application of this Regulation and promoting public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data.

(123) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should cooperate with each other and with the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation.

(124) Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union and the controller or processor is established in more than one Member State, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. It should cooperate with the other authorities concerned, because the controller or processor has an establishment on the territory of their Member State, because data subjects residing on their territory are substantially affected, or because a complaint has been lodged with them. Also where a data subject not residing in that Member State has lodged a complaint, the supervisory authority with which such complaint has been lodged should also be a supervisory authority concerned. Within its tasks to issue guidelines on any question covering the application of this Regulation, the Board should be able to issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State and on what constitutes a relevant and reasoned objection.

(125) The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process. Where the decision is to reject the complaint by the data subject in whole or in part, that decision should be adopted by the supervisory authority with which the complaint has been lodged.

(126) The decision should be agreed jointly by the lead supervisory authority and the supervisory authorities concerned and should be directed towards the main or single establishment of the controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities in the Union.

(127) Each supervisory authority not acting as the lead supervisory authority should be competent to handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involves only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees' personal data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay about the matter. After being informed, the lead supervisory authority should decide, whether it will handle the case pursuant to the provision on cooperation between the lead supervisory authority and other supervisory authorities concerned ('one-stop-shop mechanism'), or whether the supervisory authority which informed it should handle the case at local level. When deciding whether it will handle the case, the lead supervisory authority should take into account whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it in order to ensure effective enforcement of a decision vis-à-vis the controller or processor. Where the lead supervisory authority decides to handle the case, the supervisory authority which informed it should have the possibility to submit a draft for a decision, of which the lead supervisory authority should take utmost account when preparing its draft decision in that one-stop-shop mechanism.

(128) The rules on the lead supervisory authority and the one-stop-shop mechanism should not apply where the processing is carried out by public authorities or private bodies in the public interest. In such cases the only supervisory authority competent to exercise the powers conferred to it in accordance with this Regulation should be the supervisory authority of the Member State where the public authority or private body is established.

(129) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, and without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Such powers should also include the power to impose a temporary or definitive limitation, including a ban, on processing.

Member States may specify other tasks related to the protection of personal data under this Regulation. The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in Member State procedural law, such as the requirement to obtain a prior judicial authorisation. Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to Member State procedural law. The adoption of a legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision.

(130) Where the supervisory authority with which the complaint has been lodged is not the lead supervisory authority, the lead supervisory authority should closely cooperate with the supervisory authority with which the complaint has been lodged in accordance with the provisions on cooperation and consistency laid down in this Regulation. In such cases, the lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority with which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority.

(131) Where another supervisory authority should act as a lead supervisory authority for the processing activities of the controller or processor but the concrete subject matter of a complaint or the possible infringement concerns only processing activities of the controller or processor in the Member State where the complaint has been lodged or the possible infringement detected and the matter does not substantially affect or is not likely to substantially affect data subjects in other Member States, the supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of this Regulation should seek an amicable settlement with the controller and, if this proves unsuccessful, exercise its full range of powers. This should include: specific processing carried out in the territory of the Member State of the supervisory authority or with regard to data subjects on the territory of that Member State; processing that is carried out in the context of an offer of goods or services specifically aimed at data subjects in the territory of the Member State of the supervisory authority; or processing that has to be assessed taking into account relevant legal obligations under Member State law.

(132) Awareness-raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as natural persons in particular in the educational context.

(133) The supervisory authorities should assist each other in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market. A supervisory authority requesting mutual assistance may adopt a provisional measure if it receives no response to a request for mutual assistance within one month of the receipt of that request by the other supervisory authority.

(134) Each supervisory authority should, where appropriate, participate in joint operations with other supervisory authorities. The requested supervisory authority should be obliged to respond to the request within a specified time period.

(135) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for cooperation between the supervisory authorities should be established. That mechanism should in particular apply where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States. It should also apply where any supervisory authority concerned or the Commission requests that such matter should be handled in the consistency mechanism. That mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

(136) In applying the consistency mechanism, the Board should, within a determined period of time, issue an opinion, if a majority of its members so decides or if so requested by any supervisory authority concerned or the Commission. The Board should also be empowered to adopt legally binding decisions where there are disputes between supervisory authorities. For that purpose, it should issue, in principle by a two-thirds majority of its members, legally binding decisions in clearly specified cases where there are conflicting views among supervisory authorities, in particular in the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned on the merits of the case, in particular whether there is an infringement of this Regulation.

(137) There may be an urgent need to act in order to protect the rights and freedoms of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. A supervisory authority should therefore be able to adopt duly justified provisional measures on its territory with a specified period of validity which should not exceed three months.

(138) The application of such mechanism should be a condition for the lawfulness of a measure intended to produce legal effects by a supervisory authority in those cases where its application is mandatory. In other cases of cross-border relevance, the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned should be applied and mutual assistance and joint operations might be carried out between the supervisory authorities concerned on a bilateral or multilateral basis without triggering the consistency mechanism.

(139) In order to promote the consistent application of this Regulation, the Board should be set up as an independent body of the Union. To fulfil its objectives, the Board should have legal personality. The Board should be represented by its Chair. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of the head of a supervisory authority of each Member State and the European Data Protection Supervisor or their respective representatives. The Commission should participate in the Board's activities without voting rights and the European Data Protection Supervisor should have specific voting rights. The Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting cooperation of the supervisory authorities throughout the Union. The Board should act independently when performing its tasks.

(140) The Board should be assisted by a secretariat provided by the European Data Protection Supervisor. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation should perform its tasks exclusively under the instructions of, and report to, the Chair of the Board.

(141) Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

(142) Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects. A Member State may provide for such a body, organisation or association to have the right

to lodge a complaint in that Member State, independently of a data subject's mandate, and the right to an effective judicial remedy where it has reasons to consider that the rights of a data subject have been infringed as a result of the processing of personal data which infringes this Regulation. That body, organisation or association may not be allowed to claim compensation on a data subject's behalf independently of the data subject's mandate.

(143) Any natural or legal person has the right to bring an action for annulment of decisions of the Board before the Court of Justice under the conditions provided for in Article 263 TFEU. As addressees of such decisions, the supervisory authorities concerned which wish to challenge them have to bring action within two months of being notified of them, in accordance with Article 263 TFEU. Where decisions of the Board are of direct and individual concern to a controller, processor or complainant, the latter may bring an action for annulment against those decisions within two months of their publication on the website of the Board, in accordance with Article 263 TFEU. Without prejudice to this right under Article 263 TFEU, each natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, the right to an effective judicial remedy does not encompass measures taken by supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with that Member State's procedural law. Those courts should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them.

Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings before the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law, including this Regulation. Furthermore, where a decision of a supervisory authority implementing a decision of the Board is challenged before a national court and the validity of the decision of the Board is at issue, that national court does not have the power to declare the Board's decision invalid but must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU as interpreted by the Court of Justice, where it considers the decision invalid. However, a national court may not refer a question on the validity of the decision of the Board at the request of a natural or legal person which had the opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down in Article 263 TFEU.

(144) Where a court seized of proceedings against a decision by a supervisory authority has reason to believe that proceedings concerning the same processing, such as the same subject matter as regards processing by the same controller or processor, or the same cause of action, are brought before a competent court in another Member State, it should contact that court in order to confirm the existence of such related proceedings. If related proceedings are pending before a court in another Member State, any court other than the court first seized may stay its proceedings or may, on request of one of the parties, decline jurisdiction in favour of the court first seized if that court has jurisdiction over the proceedings in question and its law permits the consolidation of such related proceedings. Proceedings are deemed to be related where they are so closely connected that it is expedient to hear and determine them together in order to avoid the risk of irreconcilable judgments resulting from separate proceedings.

(145) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority of a Member State acting in the exercise of its public powers.

(146) The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice

to any claims for damage deriving from the violation of other rules in Union or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. Where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor which has paid full compensation may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.

(147) Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council[12] should not prejudice the application of such specific rules.

(148) In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.

(149) Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation. However, the imposition of criminal penalties for infringements of such national rules and of administrative penalties should not lead to a breach of the principle of ne bis in idem, as interpreted by the Court of Justice.

(150) In order to strengthen and harmonise administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. The consistency mechanism may also be used to promote a consistent application of administrative fines. It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other penalties under this Regulation.

[12] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

(151) The legal systems of Denmark and Estonia do not allow for administrative fines as set out in this Regulation. The rules on administrative fines may be applied in such a manner that in Denmark the fine is imposed by competent national courts as a criminal penalty and in Estonia the fine is imposed by the supervisory authority in the framework of a misdemeanour procedure, provided that such an application of the rules in those Member States has an equivalent effect to administrative fines imposed by supervisory authorities. Therefore the competent national courts should take into account the recommendation by the supervisory authority initiating the fine. In any event, the fines imposed should be effective, proportionate and dissuasive.

(152) Where this Regulation does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of this Regulation, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties, criminal or administrative, should be determined by Member State law.

(153) Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation. The processing of personal data solely for journalistic purposes, or for the purposes of academic, artistic or literary expression should be subject to derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, as enshrined in Article 11 of the Charter. This should apply in particular to the processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures which lay down the exemptions and derogations necessary for the purpose of balancing those fundamental rights. Member States should adopt such exemptions and derogations on general principles, the rights of the data subject, the controller and the processor, the transfer of personal data to third countries or international organisations, the independent supervisory authorities, cooperation and consistency, and specific data-processing situations. Where such exemptions or derogations differ from one Member State to another, the law of the Member State to which the controller is subject should apply. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.

(154) This Regulation allows the principle of public access to official documents to be taken into account when applying this Regulation. Public access to official documents may be considered to be in the public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary reconciliation with the right to the protection of personal data pursuant to this Regulation. The reference to public authorities and bodies should in that context include all authorities or other bodies covered by Member State law on public access to documents. Directive 2003/98/EC of the European Parliament and of the Council[13] leaves intact and in no way affects the level of protection of natural persons with regard to the processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in this Regulation. In particular, that Directive should not apply to documents to which access is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been provided for by law as being incompatible with the law concerning the protection of natural persons with regard to the processing of personal data.

(155) Member State law or collective agreements, including 'works agreements', may provide for specific rules on the processing of employees' personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee, the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by

[13] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (OJ L 345, 31.12.2003, p. 90).

collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

(156) The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials.

(157) By coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services. In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law.

(158) Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons. Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Member States should also be authorised to provide for the further processing of personal data for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes, genocide, crimes against humanity, in particular the Holocaust, or war crimes.

(159) Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures.

(160) Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.

(161) For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council[14] should apply.

(162) Where personal data are processed for statistical purposes, this Regulation should apply to that processing. Union or Member State law should, within the limits of this Regulation, determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality. Statistical purposes mean any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results. Those statistical results may further be used for different purposes, including a scientific research purpose. The statistical purpose implies that the result of processing for statistical purposes is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person.

(163) The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in accordance with the statistical principles as set out in Article 338(2) TFEU, while national statistics should also comply with Member State law. Regulation (EC) No 223/2009 of the European Parliament and of the Council[15] provides further specifications on statistical confidentiality for European statistics.

(164) As regards the powers of the supervisory authorities to obtain from the controller or processor access to personal data and access to their premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy. This is without prejudice to existing Member State obligations to adopt rules on professional secrecy where required by Union law.

(165) This Regulation respects and does not prejudice the status under existing constitutional law of churches and religious associations or communities in the Member States, as recognised in Article 17 TFEU.

(166) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission. In particular, delegated acts should be adopted in respect of criteria and requirements for certification mechanisms, information to be presented by standardised icons and procedures for providing such icons. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

(167) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011. In that context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

---

[14] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (OJ L 158, 27.5.2014, p. 1).

[15] Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (OJ L 87, 31.3.2009, p. 164).

(168) The examination procedure should be used for the adoption of implementing acts on standard contractual clauses between controllers and processors and between processors; codes of conduct; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country, a territory or a specified sector within that third country, or an international organisation; standard protection clauses; formats and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules; mutual assistance; and arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board.

(169) The Commission should adopt immediately applicable implementing acts where available evidence reveals that a third country, a territory or a specified sector within that third country, or an international organisation does not ensure an adequate level of protection, and imperative grounds of urgency so require.

(170) Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural persons and the free flow of personal data throughout the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(171) Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/ EC remain in force until amended, replaced or repealed.

(172) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 7 March 2012[16].

(173) This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council[17], including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation.

[16] OJ C 192, 30.6.2012, p. 7.

[17] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

Sheppard Mullin Privacy & Cybersecurity Team

Our group includes some of the most respected lawyers in the privacy space, including a former U.S. Department of Homeland Security deputy general counsel, a lawyer who literally "wrote the book" on data breach, award-winning privacy class action litigation practitioners, and leading EU-based data protection experts. Our accolades include being highly ranked by both Legal 500 USA (Cyber Law) and Legal 500 Europe (EU Data Protection), and one of only 25 firms ranked in the inaugural ATL Top Law Firm Privacy Practice Index.

We recognize that nearly every facet of a company's operations—from internal employment practices to online operations, data collection and customer contact— is subject to a complex array of legal and business challenges related to privacy. We pride ourselves on providing clients with practical advice from experienced counsel who thoroughly understand privacy law. Our work takes into account the global privacy and security issues faced by our clients, recognizing and respecting regional differences that reflect vastly different consumer perceptions of privacy.

As part of our work, we partner with clients to help them extract value from the data they collect, while identifying and addressing regulatory compliance requirements, and ensuring that data is appropriately protected. Our lawyers have experience responding to high-profile data breaches, and the regulatory investigations, Congressional oversight, and litigation that often follow such incidents. We also provide strategic counsel to help companies understand emerging developments in this rapidly changing area of law. Finally, as data becomes more entwined with the enterprise value of businesses, we conduct data and privacy compliance due diligence in connection with mergers and acquisitions and other corporate and strategic transactions.

SheppardMullin

GDPR AND U.S. STATES' GENERAL PRIVACY LAWS DESKBOOK