SheppardMullin

Checklist

Privacy and Data Security Considerations for Mergers & Acquisitions Deals

Privacy and cybersecurity has long been an important consideration for corporate mergers and acquisitions. How can you ensure that the privacy and cybersecurity diligence process runs smoothly throughout the process?

Getting Started

- What is the structure of the deal?
- What industry is the target in, any potential risks inherent in business?
- Whose personal information might the target collect (employee, consumer, etc.)?
- What is jurisdictional and substantive scope of review (US, EU, state laws, industry specific, activity based)?

- Will the target continue to operate independently post-transition? Or will it be integrated into the buyer's current operations?
- Will there be a transition period, and if so, what personnel or processes might need to continue post transition?
- How will personal information be used post-transaction (does buyer want to make different uses than are being made currently)?
- Will there be deal insurance?

Conducting Diligence

- What policies, procedures, playbooks, and SOPs are in place?
- What measures are in place to ensure adherence to those policies?
- What other documentation does the target have about its data use activities?

- Is the target engaging in any regulated or highly-litigated activities, and if so, is it compliant with relevant laws?
- Does target hold or process any sensitive personal information (if so what, and how is it used? Is use compliant with applicable laws? Any other risks)?
- Have you obtained a clear understanding of how the target processes personal information for each category of individuals on whom it maintains information?

More Diligence Concerns

- Does the target have data maps or other schematics that shows what personal information it holds? Do those records explain how the target uses personal information?
- Is the target using third party resources or tools in the processing or protection of its personal information?
- Do any vendors (especially critical vendors) have security risks that may impact target?
- Does the target make any promises about data use (privacy) or security in its contracts with third parties?
- Are there any jurisdictional-based restrictions on data transfers, including cross-border transfers, that might be triggered by the deal (especially asset structured deals)?

Is the target (or seller) in a regulated industry or subject to privacy or data security laws that might impact data transfers or new uses of personal information post-closing?

Has the target suffered a data breach or other data incident?

Did it follow notice obligations? Is there potential litigation risk that may arise post-closing? Does it have cyber insurance that covers incidents, and will coverage last post-closing?

Are technologists conducting a review? Have they identified any significant red-flag gaps?

Pre-Closing Considerations

- Were there any red-flag risks that may impact the deal (can those be addressed with an indemnity or will it impact valuation)?
- Did the diligence identify any pre-closing remediation needs (any restrictions on data transfers in agreements or privacy policy, for example, for asset deals)?
- Does the buyer need a remediation gap assessment conducted (useful for planned integration)?
- Are there items that should be identified for post-closing remediation?
- Will there be any disruptions in data availability during the closing period or after?
- Did diligence uncover any hindrances on buyer's potential ability to use the acquired personal information?
- Did diligence impact any of the deal documents? Anything that needs to be scheduled?
- Will data protection regulatory notifications be needed (for example in jurisdictions where DPO/database registration is required)?
- Do the parties want to share personal information before the deal closes (and if so, what structure, agreements, or consents might be needed)?

Post-Closing Activities

- Will any of the target's employees or processes be used during a transition period (do any access protocols need to be changed as a result? Consulting relationships?)?
- Has an integration plan been developed for both data and systems (does the buyer have an integration playbook; issues include data harmonization, systems integration, networks, messaging systems, security, etc.)?
- Will the target's personal information be integrated into the buyer's systems?
- Will data be offshored (or if offshored, will it be transferred across borders)?
- Will there be changes to the target's existing policies and procedures, and/or will they need to adopt the buyer's policies and procedures?

- Will any vendor relationships be terminated (for example because it will be replaced with buyer's vendors)?
- Does an intragroup transfer agreement need to be updated to reflect the target's membership in the seller's business?
- Have appropriate notices and consents been obtained where needed for new uses of target's CRM data?
- Will target's data be cleansed, augmented or otherwise modified?
- Will any of the target's business operations cease? If so what will be the impact on personal information (do impacted individuals need to be notified? If data is being destroyed, what measures are in place to do so securely)?

This checklist was prepared by Sheppard Mullin's Privacy and Cyber Security Team, a multi-disciplinary practice whose members include some of the most respected lawyers in the field. This resource is prepared as a courtesy for our clients and is not intended to serve as or replace legal advice. You should contact your regular Sheppard Mullin contact or one of our privacy team members with questions (for more information visit www.sheppardmullin.com/privacy-and-cybersecurity).