GDR NEWS

How to take a holistic approach to privacy compliance in an ever-changing legal landscape

14 January 2021

Sheppard Mullin Richter & Hampton privacy and cybersecurity practice group leader **Liisa Thomas** lays out how companies can best comply with global data privacy laws in uncertain times.

Most of us were happy to see the end of the year 2020. Companies have faced untold challenges, and so have their personnel. In several years, we may have the luxury of looking back at this time as one of opportunity and growth. Seeing that benefit now, however, is a challenge. Easy wins and silver linings may not be obvious, especially when we think about privacy and data security.

First published on the *Global Data Review* website, January 2021

There are some things that we can glean from privacy trends over the last few years (including this unusual one). Which trends? There are several, including the changing landscape of international data flows; a more general effort by companies to map and understand the flow of personal information between them and other companies; ongoing enforcement action; the stops and starts companies have felt in preparing for laws that are about to go into effect – and then do not; and finally, the resurgence of enforcement around laws that many of us may have forgotten about.

All of these trends have a common theme: uncertainty and instability. That type of environment can be particularly hard to prepare for if a technical approach, as opposed to an adaptive approach, is taken.

How, then, can companies face this uncertain world? As the legal landscape becomes more complex, it becomes more important that any approach be a holistic one. There is nothing worse than spending time and effort on compliance efforts around one law, or set of laws, only to have those laws modified – or to have new laws pass just as a company completes its change efforts.

It is all well and good to say that your compliance approach should be holistic, but what does that mean? And how does one create such an approach in the face of an ever-changing privacy landscape? There are several steps will stand corporations in good stead:

Start at the beginning, not the middle. Too often privacy teams attempt to implement new policies and procedures before conducting sufficient diligence. Not just diligence about existing practices, but more fundamentally, thinking through *how* to get any policies and practices implemented into the company's culture. What is the corporate culture? Risk adverse? Transparent? How are significant changes made? Are there key stakeholders that will need to be won over before any compliance modifications are successful? Taking the time to think through how to make change, and what change will look like, before implementing it is critical. With this, the privacy team can develop a privacy compliance approach that is better integrated into the corporation, and can more easily change and grow as laws are modified.

Include the right people in diligence efforts. When working on understanding the company's goals and needs – as well as its current information and use practices –

the right people need to be in the room. Those who can best describe not only *where* information is housed, but also *why* the company has that information and *how* it uses the information. What is the business purpose for collecting it? What are current and future plans for its use? Marketing, sales, e-commerce and digital teams typically need to be involved in these discussions – not just the information technology and security departments.

Remember your partners. Your business teams work with a myriad of other companies. Whether they are vendors, clients, or others, information often flows between your company and others. Thinking through not just the technical side of how information gets to those partners, but also *why* it is going to those partners (or from those partners back to you) is critical. It will help you identify any security remediation steps you want to take, and will also help you with priority levels. Data transfers that are happening because they support fundamental business processes will take precedent over those that are not mission-critical.

Remediate and change intelligently. As the privacy office learns more about current and future data use practices, there may be a knee-jerk desire to launch multiple policies – an attempt to solve a technical problem when a broader approach is needed.Think carefully about what policies are the right ones for you, and how you will disseminate and train around them. It's rare that drafting and publishing an internal policy will be sufficient to effectuate compliance. You will have to win over hearts and minds as well. Having a clear picture of how you will accomplish that will mean your policies and the underlying privacy compliance approach are that much stronger.

Train with an eye towards measurement. Nothing causes more angst to a compliance professional than hearing that employees continue to do the exact opposite of what was covered in extensive training sessions. When developing privacy training, think about not just who needs to receive training (those who collect, use or interact with personal information), but also how best to change their behaviors. Training may need to be tailored not only to the types of activities in which different teams engage, but also to their learning styles. The training for the sales team will look different than the training for the digital, social media, or e-commerce teams, even if the substantive message is the same.

Don't set it and forget it. Your company's information practices will change. Your personnel will change. As you go through the prior steps, companies will be well served to think about how to incorporate not just specific activities but the importance of privacy within the company. Stakeholders may need to be won over, and cultural change may be needed.

First published on the *Global Data Review* website, January 2021

As companies continue to mature their privacy compliance approach, they will face ongoing changes and enforcement. To be prepared, they can take advantage of holistic steps, including starting at the beginning, not the middle, remember partners, being adaptive not technical, training appropriately, and not “setting and forgetting.” These are just a few things that can start your year well, even if 2021 brings more of what we have seen in 2020.

First published on the *Global Data Review* website, January 2021