KILPATRICK TOWNSEND

5 KEY TAKEAWAYS

Building a Strategic Privacy Program

The responsibilities of privacy professionals continue to grow while resources are increasingly difficult to procure. At the Privacy + Security Forum, the deeply experienced panel of privacy professionals consisting of Ami Rodrigues of Chipotle Mexican Grill, Inc., Christina McCoy of Acoustic, Evan Glover of NCR and Amanda Witt of Kilpatrick Townsend & Stockton LLP shared suggestions on how to build and maintain a strategic privacy program with limited resources while still ensuring that such program is designed to comply with the ever-growing web of complex privacy legal obligations.

The key takeaways from this presentation were as follows:

1

Reframe the challenge of building a privacy program to view it as an opportunity to differentiate your organization from its competitors. Implementing stronger privacy protections is a way to build trust with your customers. By being compliant with global privacy regimes, you're creating expansion opportunities for your organization. Those organizations who have designed their privacy programs to be compliant with the EU's General Data Protection Regulation (GDPR) have more easily adapted to meet the challenges of increased US legislation as well as new international privacy laws such as the LGPD in Brazil. Furthermore, having the ability to demonstrate a mature privacy program can lead to additional business from sophisticated business customers who are looking for vendors who value privacy.

2

Look for opportunities to harmonize across jurisdictions by finding common principles in the various laws. If a privacy program is organized across common themes present in various privacy laws (e.g., transparency, data subject rights, breach notification, privacy by design, DPO designation, etc.), it is easier to adapt to new privacy laws. Beginning with the GDPR, the laws that have followed in the United States and globally have expanded individual rights to data, included enhanced transparency requirements and imposed additional obligations for the protection of data throughout the supply chain. By organizing a privacy program around the commonalities of these laws, it makes your program more agile and makes it easier to adapt to new laws.

3

Understand your customers, your organization and data flows when designing your privacy program. To know your compliance obligations, you'll need to understand the types of data you're collecting and your organization's data flows. It will be important to determine whether you're collecting the personal information of consumers or if your business primarily collects business-related (i.e., B2B) data. You'll also need to understand your organization's risk profile, willingness to accept risk and prior experience with privacy or security incidents or enforcements. Lastly, it is also important to determine the impact that compliance may have on the organization and the speed (and/or willingness) in which the organization can implement necessary changes.

4

Educate the leadership of your organization so that they understand the risks. C-suites and Board of Directors often push the organization for cost reductions, elimination of redundancies, and creation of valuable insights—and for people to accomplish more with less. Inefficient implementation of compliance requirements and responsibilities, however, leads to risk and/or compliance fatigue. It will be important to effectively communicate the benefits of compliance and the risks of non-compliance. It may help leadership understand privacy risk if such risks are tied to or compared with other enterprise risks. Competition can be used as a motivator in some circumstances if leadership can be persuaded that privacy compliance is a way to differentiate itself from its competitors.

5

Effectively communicate the success of the program to leadership. Managers of privacy programs are often asked by leadership to show the return on investment (ROI) of a privacy program. The panelists shared ways in which they demonstrate the benefits of their privacy program including by benchmarking the program against third party standards (e.g., ISO, NIST, etc.) or showing cost-savings obtained by streamlining processors and vendors. Ideally, to continue to receive the support of leadership, it is important to communicate successes to leadership at least annually. Such successes could include compliance with a new law or opening up a new territory for expansion.

For more information, please contact:
Amanda Witt: awitt@kilpatricktownsend.com

www.kilpatricktownsend.com