Published on *The National Law Review* https://natlawreview.com

What Does an Adaptable Privacy Program Look Like?

Article By:

Liisa M. Thomas

Privacy professionals know “adaptable” programs are important. But what does that really mean? What does it look like? And how do we create one? We know that with the never-ending list of new laws and modifications to existing laws, being adaptable is key. To say nothing of regulatory enforcement and class action exposure. The following are ideas to help create -or modify- your program to be adaptable in face of the constantly changing privacy patchwork.

1. Align With Corporate Mission

There is nothing worse than spending time, energy and funds on a privacy program, only to find leadership unwilling to fund or adopt it. Before beginning your work, think about your organization’s underlying mission. How can the privacy program support that mission? If your program aligns with the needs of the organization, you are more likely to get leadership buy in, and sufficient personnel, technology, financial and other support to make the program a reality. Many tools exist for aligning your program with your corporation’s mission, including Balanced Scorecard work from Robert Kaplan and David Norton.

2. Appropriately Identify and Categorize Risks

“Be prepared” has become a buzzword for regulators and legislators. There is a growing expectation from both legislators and regulators that the corporate world will identify and prepare for risks. However not all risks are alike. Some risks, as Robert Kaplan and Anette Mikes tell us, are unknowable and unexpected. These could be novel cyberattacks, or new laws that regulate activities in ways not previously seen. Policies alone may not prepare a company for these risks. Instead, think about how train teams to work together in new circumstances. Tabletops that focus on teamwork, rather than preparation for a particular fact pattern, can be helpful.

3. Don’t Over-Engineer: Make it Strategic

Obviously, a privacy program will need to address the laws and legal risks. It will also need to take into account the growing and complex matrix of third parties with whom organizations work. However a strategic program does not necessarily have to take a scorched-earth approach. In fact, many have found this makes implementation impossible. Instead, an adaptable program addresses the organization’s business needs and risks. It takes into account the changing nature of privacy and data security laws and risks and builds in mechanisms to review and revise. For example, frameworks against which new programs or processes can be audited. Or, personnel within different business units that serve as “champions” of privacy: both bubbling up concerns to central privacy teams and spreading knowledge about obligations to their business team constituents.

4. Customize to Your Organization

An adaptable privacy program is one that has been adapted to the company. While informed by external requirements and risks, it is also informed by internal activities. Privacy policies, for example, describe the *company’s* activities. Data protection protocols protect the company against risks *it* faces. Additionally, the program includes a process for ensuring compliance with those processes and procedures. It is an implementable plan that avoids being overly aspirational. It is easily understandable by the business and thus one to which employees can adhere. A place to start might be a standard SWOT analysis, identifying gaps between the current program and the company’s mission, as well as gaps in addressing risks facing the company. Those opportunities can then inform a list of remediations – including personnel and technology support.

5. Use Change Management: Celebrate Small Wins

Finally, an adaptable program takes into account not just written policies and procedures, but the personnel who will be implementing and following those documents. To the extent that the documents place new expectations or restrictions on individuals, these changes may be resisted. Privacy professionals would thus be well served to borrow pages from change management, thinking about the traditional “freeze, change, refreeze” triad from Karl Lewin. Or, from John Kotter, create urgency, a coalition, a vision, an implementation army, remove barriers and importantly: celebrate small wins. This last can keep motivation going, especially when getting to the end, instituted change, is hard. Or, when as with privacy, once reaching the end, one needs to restart as the privacy patchwork has shifted!

Putting It Into Practice: As the privacy patchwork continues to develop and shift, the need for adaptable programs becomes all the more critical. These five suggestions are based on both legal and regulatory risks. They are also informed by the teachings of change management, something privacy professionals might overlook when building their privacy program toolbox.

Listen to this post

National Law Review, Volume XIV, Number 165

Source URL:https://natlawreview.com/article/what-does-adaptable-privacy-program-look