BEYOND COMPLIANCE: EIGHT STEPS FOR USING PRIVACY BY DESIGN TO DEVELOP A PRIVACY PROGRAM

ELSE KHOURY

Governments globally are passing strict information privacy laws and regulations, and organizations are being hard-pressed to comply with them or suffer stiff penalties. Using the principles of Privacy By Design, organizations can design a privacy program to meet this challenge.

Mandatory privacy breach reporting. Privacy impact assessments. Access to information requests. The right to be forgotten. If these terms, which pop up in regulations like the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act, and Canada's Personal Information Protection and Electronic Documents Act strike fear in your organization, it's not alone. Identity theft, reputational damage, and class action law suits are just some of the known results of data breaches.

UNDERSTANDING PRIVACY IMPACTS

In 2013, when Edward Snowden revealed the extent of government surveillance over private citizens by the U.S. National Security Agency, the conversation about privacy began its slow crawl from the tin-foil-hatted conspiracy theorists hiding in off-the-grid cabins to the average suburban living room. Suddenly, regular citizens were beginning to question the extent of their vulnerability and the vast amounts of personally identifiable information (PII) they have given away, willingly or not. Six years later, questions on privacy and security increasingly demand attention. The privacy conversation has even permeated the pop culture bubble: where would the plot lines of television's "Mr. Robot" or the Bourne movie trilogy be without it?

Adding fuel to the fire, an abundance of global data breaches has exploded, taking corporate bottom lines and personal privacy down with them. While the Equifax, Yahoo, and Ashley Madison breaches resulted in heavy losses to their parent companies and damage to the vendor-client relationships, it is easy to lose sight of the fact that privacy breaches cause real, individual, human harm. In Canada alone, two individuals affected by the 2015 Ashley Madison breach were known to have taken their lives immediately after client data was posted online: in a very real sense, privacy breaches ruin lives.

Against this backdrop is an evolution in the general public's understanding of and demand for privacy rights. Both the UN Declaration of Human Rights and the International Covenant on Civil and Political Rights recognize privacy as a basic human right. Some argue that without the right to privacy, other rights are moot. Globally, governments have been seeking to create or amend their own privacy legislative frameworks in response to the changing landscape of digital data and risks associated with conducting business on the Internet.

While the introduction of new laws certainly increases accountability, for organizations unused to a framework of rigorous privacy compliance requirements, the demands can feel overwhelming. But the alternatives are worse: with fines of up to 2% of annual turnover under the GDPR, non-compliance is a non-option.

PUSHING PAST COMPLIANCE

Privacy compliance requirements, with their complex accountability structures and processes, require a great deal of time and consideration to implement. The question then becomes: How can an average organization improve privacy compliance without shutting down business or placing a complete stranglehold on productivity?

Perhaps the best way to get started is to take the view that compliance is a continuous process of change, not a singular effort like developing a privacy officer position or drafting a privacy policy. To ensure that compliance happens, privacy needs to be addressed as an ongoing, corporate-wide,

behavioral shift. Fortunately, there is a methodology that can help organizations get to compliance, and even push past it by integrating its principles into the organization's culture.

USING PRIVACY BY DESIGN

Privacy By Design is the brainchild of Ann Cavoukian, Ph.D., Distinguished Expert-in-Residence and Leader of the Privacy By Design Centre of Excellence at Ryerson University in Toronto, Canada. "Privacy By Design was developed at my kitchen table," Cavoukian recalls of her time as Ontario's information and privacy commissioner. "I wanted to find a way to build privacy into the design stages of technology."

Privacy By Design was a revolutionary concept when it was unveiled by the Office of the Information and Privacy Commission during Cavoukian's tenure. It's a surprisingly accessible methodology that focuses on balancing productivity with the end goal of protecting privacy, in what Cavoukian has repeatedly described as the "positive sum" paradigm. "Privacy By Design takes a positive-sum position in order to accommodate all legitimate interests," she said. "We don't talk about privacy versus security, for example, but how to accommodate both."

Creators of the GDPR used Privacy By Design as a foundational principle when developing the regulation, and the same approach can be applied in an organization that is attempting to become privacy compliant. Privacy By design focuses on a preventative approach, which is probably the greatest shift an organization will have to make: thinking about putting privacy-protective measures in place before something bad happens. If an organization is really committed to ensuring that it doesn't end up as a national headline, this is where it needs to start: establishing a privacy compliance infrastructure that develops the tools necessary to take the organization to compliance and beyond.

BUILDING A COMPLIANCE INFRASTRUCTURE

Building a privacy compliance infrastructure requires organizations to take the following eight actions:

1. UNDERSTAND REGULATORY / COMPLIANCE OBLIGATIONS

Before looking at implementing any kind of privacy program, an organization needs to understand what its obligations are. This begins with a simple question: What enables the organization to do what it does? In health care, for example, there are regulations or standards that define the boundaries of the services an organization provides, such as vaccinations or palliative care. These laws define the limits of service, which means the organization can collect, use, share, store, and eventually destroy information only for those purposes. This is called consistent purpose, and it is the basis for all further privacy considerations. Any information that that does not fulfill that purpose has no place in the organization unless it has been collected with the information subject's consent.

2. IDENTIFY THE ORGANIZATION'S INFORMATION AND WHERE IT'S LOCATED

It is imperative for an organization to ensure that it doesn't have PII that does not meet the definition of consistent purpose. This can be tricky; in the age of mass data proliferation, many organizations do not have a complete view of the PII they hold or where it is located.

But, organizations can't begin to implement protections on personal data until they know where to find it. There are many tools available to help identify and locate digital information, but organizations must "go deep" to ensure that they have considered information in all formats, including paper.

3. GAIN EXECUTIVE SUPPORT

The role of management is fundamental in ensuring the success of any privacy program. Unless the organization's board of directors or executive management team has vocally confirmed its commitment to privacy, it's likely that compliance at other levels of the organization will be sub-par. That commitment must be demonstrated by executive management's funding, championing, and participating in the privacy program; they need to walk the walk. A privacy program without devoted staff and a budget is doomed to fail.

4. ESTABLISH ACCOUNTABILITY FOR THE PROGRAM

To be clear, efforts toward implementing an infrastructure of privacy compliance will not work without accountability being established. At the bare minimum, an organization must identify a privacy officer (called a data protection officer or DPO under GDPR) or someone else who holds accountability for privacy within the organization. But accountability should not be limited to a single individual who receives and processes privacy complaints; it extends to every individual who interacts with any piece of information that could meet the definition of PII, which includes any of the following:

- Contact information (address, telephone number, email address)
- Employment history
- Gender, race, religion
- Financial information
- Medical information

This means staff in human resources, finance, client relations (depending on what the organization does), and probably other departments have accountability for privacy.

Considering the extent to which personal information may be collected, used, shared, and stored in the organization, what privacy compliance considerations have been put in place? Does the organization conduct regular privacy training by an experienced professional familiar with the compliance landscape? Once that training has been completed, has staff undergone testing to ensure that they understand their responsibilities? Are policies and procedures in place to deal with, among other things, privacy audits and a privacy breach response?

5. DEVELOP POLICY AND TRAINING

It's basic, but it works: developing policies and standards of practice, building privacy into processes, and providing context and direction to all staff are imperative to the success of a privacy program. The key is to make sure that the right information is delivered to the right people. Target the information to the audience, make it useful for them, and follow training with testing (with recorded results) and annual policy review.

6. ENSURE THIRD-PARTY COMPLIANCE

"You can't outsource accountability," Cavoukian said about third-party handling of PII. All third parties that have access to an organization's PII must be made aware of any privacy obligations the organization has and should be required through contracts and agreements to honor those obligations. To help ensure compliance, be transparent about these obligations by building privacy requirements into the scoring stage of the procurement process.

7. INTEGRATE THE PROGRAM INTO GOVERNANCE

Finding a prominent place for the program within the organization is critical for privacy compliance. Senior management should provide the support to ensure that privacy is woven into the fabric of your organization. Without a seat at the right tables, the accountable people may not be aware of new initiatives or projects that contain a privacy risk element.

8. IMPLEMENT PRIVACY IMPACT ASSESSMENTS AND MITIGATION PLANS

Privacy impact assessments (referred to as Data Privacy Impact Assessments in the GDPR) are still the most effective (albeit time-consuming) methods to prevent privacy risks from manifesting in organizations. Together with the infrastructure elements listed above, they will complete a privacy program.

If a privacy breach should occur, an organization must have a formal response in place to contain the damage and control the messaging afterward. As the last line of defense, a strong privacy response plan will doubtlessly save an organization from the misery of the having the breach discovered and disclosed by a member of the public – or worse, by the media.

PUTTING IT ALL TOGETHER

Putting a strong and effective privacy program in place is no mean feat. It requires ongoing time, commitment, and support. By using the principles of Privacy By Design as a model, an organization can break down the necessary steps to reach – and push past – compliance.

about the author

Else Khoury

Else Khoury is the Deputy Clerk at The Township of West Lincoln in Ontario, Canada, an instructor at the University of Toronto School of Continuing Studies, as well as Principal Consultant at Seshat Information Consulting