ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Maturing Your Organization’s Privacy Program

Technology, Privacy, and eCommerce

Banner artwork by Suttipun / *Shutterstock.com*

The scope of privacy professionals is broad. The adoption of privacy policies and procedures, privacy training and communications, deployment of privacy and security-enhancing controls, management of third parties that process personal information and the assessment of compliance with regulations and established control mechanisms all fall under the remit of privacy professionals, who are often in-house counsel. *Privacy Program Management, Tools for Managing Privacy Within Your Organization*, 3rd Edition, is an extremely useful publication of the International Association of Privacy Professionals (IAPP), which outlines the responsibilities of privacy professionals in great detail.

Developing a successful privacy program

Accountability is the most important aspect of the privacy framework. For most major organizational initiatives to be successful, there must be structure, consistency, and buy-in at the highest levels. Privacy governance is no different. A successful privacy program requires a structured team, thoughtful strategy, and supportive stakeholders who remain committed to protecting personal information throughout the data lifecycle.

A privacy program cannot be efficiently run without an organized team and plan of action. Sergey Nivens / *Shutterstock.com*

This article draws from the thoughts of three experienced privacy professionals:

Sara Azargive, director, privacy compliance and privacy counsel at the Ontario Teachers' Pension Plan

Maureen Dry-Wasson, VP, group general counsel and privacy officer at Allegis Group


Melissa Abramowitz, VP, legal and compliance officer at CAA Club Group

Their perspectives on wins, challenges, and their goals for 2023 provide insight into some of the key considerations for maturing one's privacy program.

Shift the mindset on data minimization

One way to merge compliance and strategy is to treat compliance as a baseline. The privacy program creates an opportunity for organizations to re-evaluate and improve data management practices, such as creating a data inventory or considering access rules established for different points in the data lifecycle.

> The privacy program creates an opportunity for organizations to re-evaluate and improve data management practices, such as creating a data inventory or considering access rules established for different points in the data lifecycle.

Dry-Wasson reflected that one of the most important areas of progress at Allegis Group for reducing privacy risk has been "shifting the mindset on data minimization." That is, considering what's really needed to run the business and maintaining an enforceable global record retention schedule.

Abramowitz stated this will be a key area of focus for CAA Club Group in 2023 – considering an information governance program more broadly that involves participation from the business leaders across the organization. Business leaders need to understand the value of the data they collect and

their “responsibility in making appropriate choices about its use and retention.” This should not just be a concern for privacy, compliance, and IT representatives.

Compliance should be achieved with the least amount of business disruption. It’s appropriate to consider business disruption as another form of penalty, and weigh it along with fines for non-compliance with data protection laws.

For example, Sara mentioned that it is important for her team to recognize that there will always be competing priorities. But with “creativity and innovation,” organizations can stay true to their privacy program’s mandate and ensure it continues to engage stakeholders and maintains its position when it comes to assessing key organizational risks that need to be mitigated. “Privacy by – design" is one technique for integrating compliance with organizational strategy, and this will be a key area of focus going forward for Allegis Group – Dry-Wasson suggested analyzing new initiatives with a privacy-by-design lens is imperative.

Organizational risks can be alleviated with the help of brainstorming and implementing creativity through your team. Gajus / *Shutterstock.com*

Training and awareness

Training and awareness programs can effectively communicate privacy policies and procedures. Ultimately, they serve to help change bad behaviors and reinforce good ones. Training communicates the organization’s privacy message, policies, and processes — including for data usage and retention, access control, and incident reporting.

> Training communicates the organization’s privacy message, policies, and processes —

> including for data usage and retention, access control, and incident reporting.

Awareness programs reinforce lessons through diverse methods and regular reminders. Both Azargive and Abramowitz spoke of training initiatives as being the most effective defense against privacy incidents. It is an area they felt their organizations have made significant strides forward on by focusing on training content that is interactive, engaging, and practical.

Data assessments can help track personal information and inventory, as well as determine the impact that systems and processes will have on privacy. They become increasingly important with the rapidly changing landscape that privacy professionals face.

Data assessments are vital to ensure personal information is protected. Daenin / *Shutterstock.com*

As Azargive mentioned, the use of data continues to become more “sophisticated and complicated.”

Keeping up with the business and regulations

Abramowitz also felt the most challenging aspect of her role is “keeping up with the business” in terms of identifying the privacy implications of a proposed initiative such as data analytics or the desire to use data for purposes not originally contemplated at the time of collection. And given the pace of and need for innovation, it is not just about ensuring alignment with the privacy program. Whether the program itself also needs refreshing must be considered.

> And given the pace of and need for innovation, it is not just about ensuring alignment with the privacy program. Whether the program itself also needs refreshing must be considered.

Staying on top of an organization's data analytics can be a difficult task but is paramount. Andrey_Popov / *Shutterstock.com*

Dry-Wasson framed data as an asset and a liability. In addition to leveraging data appropriately with privacy accounted for, she also highlighted rapidly changing laws as a key challenge for her role.

And with regulations lagging behind, this challenge is further aggravated. For example, the *California Privacy Rights Act* came into force January 1, 2023 but organizations are still waiting for regulations that will critically guide their compliance efforts. Not only is it difficult to stay on top of legal requirements, but sometimes the rules being developed are not business practical, highlighting the need for better partnership between government and business.

Different laws and regulations around the world may incorporate common elements, such as offering consumers notice and choice, but privacy-related tasks, such as international data transfers, can be tightly regulated and, if done improperly, can have major consequences for an organization.

Privacy compliance is a marathon, not a sprint

Based on the insights these corporate counsel graciously shared, and my own experience working within a variety of industries on data governance and privacy programs over the past 21 years, setting priorities and making best use of limited resources requires careful planning. Never a dull moment for a privacy professional in today’s data-driven economy.

Fazila Moosa

Senior Privacy Counsel and Lead Consultant

PRIVATECH

Fazila Moosa, founder of PRIVATECH, is a privacy and cybersecurity lawyer, consultant and trainer with 21 years of experience in the field, both in a large law firm environment and as an entrepreneur. She has a unique blend of legal, IT consulting, and data governance experience. Moosa advises businesses in North America in a range of industries on privacy and security best practices, and also provides direction to public sector clients on the implementation of initiatives with privacy implications.

Before founding PRIVATECH, Moosa also worked with the Office of the Privacy Commissioner of Canada, where she was heavily involved in establishing complaint-handling procedures, and assisting investigators in interpreting federal privacy laws.

Moosa holds degrees in Electrical Engineering from the University of Waterloo and Bachelor of Laws from the University of Toronto. She is a certified information and privacy professional with the International Association of Privacy Professionals (IAPP), as well as a Certified CSX (Cybersecurity) professional with the Information Systems Audit and Control Association (ISACA). Moosa has been recognized as a ‘Privacy by Design’ ambassador since 2011, is an Official Training Partner of the IAPP, and serves on the Board of Directors for Newcomer Women’s Services Toronto. Fazila Moosa can be reached at fmoosa@privatech.ca or 1-416-903-1133.