iapp

GETTING STARTED
with Privacy in Canada

Maria Koslunova, CIPP/C, CIPP/US, CIPM, PwC

Many employees, especially at medium-sized firms, get approached by their superiors asking them to wear "different hats." Lately, a lot of people have been trying privacy hats on for size. Although this may not necessarily be a problem for those of us wishing to acquire new skills, it could pose challenges for others. Particularly for individuals with limited privacy knowledge, they may not know where and/or how to start figuring out what privacy is and how it impacts their organization.

Developing and managing an organization's privacy program is a continuous journey within an ever-changing landscape. Regardless of the size of the organization, it is very important for the tasked individual to address the following key areas at the start:

- What personal information do we collect?
- What legal/regulatory/industry standards apply to us?
- What existing privacy mechanisms do we have in place?
- How do we improve?

By taking the time to address these items, an individual can develop a holistic view of what an organization is currently doing and where the struggles are. These actions make it possible for the organization to mitigate any privacy compliance risks and serve as a foundation to build the privacy program for sustainable privacy risk management over time.

1. What information do we collect?

This question is very important in the initial stages of developing a privacy program. By not being sure of what personal information is held and the purposes for which it is being used, an organization is unable to ensure that all personal information is being properly protected and used in a legally compliant way.

By completing a personal information inventory and identifying what information is collected and why, an organization is able to determine what protections need to be put in place. Once a personal information inventory is complete, it is important to start classifying all personal information into high risk, sensitive, internal, and/or public categories. High risk personal information generally requires a greater level of protection, while lower risk personal information, possibly labeled "internal," requires proportionately less. Employing a proper personal information classification scheme is crucial, as it will allow an organization to be efficient with its financial resources by focusing more protection efforts on its high risk personal information.

It is also important to identify where the organization collects the personal information from. Specifically, is the personal information collected directly from the individual(s)? Was personal information collected directly from third parties? Has individual consent been obtained for collection, use and disclosure of the personal information?

It is also important to identify where the individuals are located in order to adhere to any legal requirements. For example, the EU's General Data Protection Regulation places specific requirements on organizations processing personal information of individuals within the EU. These requirements apply regardless of where the data controllers are located in the world.

2. What legal/regulatory/industry standards apply to us?

Organizations should start by reviewing an industry standard such as the Generally Accepted Privacy Principles (GAPP). The GAPP helps to address the privacy requirements for the personal information lifecycle, including, but not limited to notice, consent, accountability, use, collection, retention, and disposal.

In addition, it helps to determine the jurisdiction and sector where the organization is operating. Specifically in Canada, personal information protection is governed by numerous laws and regulations, which can be classified into the following categories:

I. Federal legislation:

  - **a. Privacy Act:** Covers the personal information-handling practices of federal government departments and agencies.

  - **b. Personal Information Protection and Electronic Documents Act (PIPEDA):** Sets out the ground rules for how private-sector organizations collect, use, and disclose personal information in the course of commercial activities across Canada Some provinces have privacy legislation that has been deemed "substantially similar" to PIPEDA, which means that provincial legislation is applied instead of PIPEDA.

II. Provincial Legislation — Provinces with privacy legislation deemed "substantially similar to PIPEDA:

  - **a. Alberta's Personal Information Protection Act (PIPA)**

  - **b. British Columbia's Personal Information Protection Act (PIPA)**

  - **c. Québec's An Act Respecting the Protection of Personal Information in the Private Sector (Quebec Privacy Act)**

III. Provincial Health Care Privacy Legislation

  - **a. Ontario's Personal Health Information Protection Act**

  - **b. New Brunswick's Personal Health Information Privacy and Access Act**

  - **c. Newfoundland and Labrador's Personal Health Information Act**

IV. Additional regulations and best practices include:

  - **a. The Canadian Anti-Spam Legislation (CASL)** — Considered the toughest anti-spam law in the world. The law places strict requirements on the:

    - Sending of any electronic message (e.g., email, text message, social media message) that involves some form of commercial content.

    - Installing computer programs (e.g., applications) onto another user's device in the course of a commercial activity.

  - **b. Payment Card Industry Personal information Security Standard (PCI DSS)** — A proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover and JCB.

Once the applicable legislations are identified the organization will be able to identify specific requirements and how to comply to said requirements.

3. What existing mechanisms do we have in place to protect the personal information we collect?

It is important to conduct an assessment in order to understand the current state privacy practices, including how personal information flows into and out of business units and systems. By doing this, an organization is able to identify what current risks exist in comparison to legal, regulatory and industry requirements (as identified in question 2).

In most cases this can be done by assessing:

I. Existing policies and procedures, including:

- **External:** Public-facing message that communicates with customers and other stakeholders what the organization's personal information handling practices are.
- **Internal:** These are internal-facing policies that dictate the ways in which the organization collects, uses, protects and discloses personal information collected.

II. The nature of information collected, the purposes of its collection, how privacy and security are ensured operationally throughout the life cycle of the information, and what mechanisms are in place to provide individual access to information and respond to complaints and requests.

III. Privacy and security issues arising from employee awareness, management support processes, availability of guidelines and manuals, and mechanisms for communicating privacy and security practices.

IV. Existing mechanisms that are in place in order to protect personal information from unauthorized access, use and/or disclosure.

4. How do we improve?

By establishing the current state of maturity and risk baseline, the organization is able to envision its future target state based on specific regulatory requirements, business objectives and operational goals. Privacy should be considered in all business activities, with controls being designed into operations right at the beginning of every new activity.

Remember that a strong privacy foundation should include key components and capabilities, including:

I. Senior management support and commitment to the overall privacy program.

II. An accountable individual who is responsible for the privacy program.

III. Adequate internal and external policies and procedures that address legal obligations.

IV. Up-to-date training and education for all employees and tailored to specific roles.

V. Suitable security that includes administrative, technical and physical safeguards.

VI. Acceptable breach and incident management response protocols.

VII. Strategy on disclosing personal information to third parties, privacy provisions within contracts and periodic audits of third parties.

VIII. Adequate privacy program monitoring and metrics.

A privacy program is an ever-evolving process and needs to be continuously updated. Appoint accountability agents and construct governance structure in line with organization culture and requirements. Monitor and report on key performance indicators to determine effectiveness of privacy services. Obtain external assurance and guidance to assist with the organization's ever-evolving privacy journey.