INTERNAL AUDIT PERSPECTIVES

DATA PROTECTION AND PRIVACY

IAI Canada Montréal

Introduction

With the collection and processing of personal information multiplying at an unprecedented rate, privacy protection has become a major concern for individuals and organizations. Internal auditors play an essential role in ensuring that their organizations comply with privacy laws and regulations and maintain the digital trust of their stakeholders.

We interviewed Florian Strich, co-chair of the IAPP Knowledge Network Montreal chapter, to discuss these issues and best practices in privacy management within organizations.

BIOGRAPHY

Biography

Florian started his career 10 years ago as an internet law specialist after studying at the Sorbonne. He has worked on privacy issues, including the right to be forgotten and cyberbullying, in specialized law firms before returning to studies to train in computer science and business (ESSEC/Telecom Paris). As co-founder of the Information Governance Chair at ESSEC, he then moved into consulting, helping companies for the past eight years to combine privacy protection and data governance. Joining PwC five years ago, he moved to Quebec two years later to develop the French-speaking privacy practice.

Interview

01 What exactly is meant by the protection of personal information and how does it relate to digital trust?

The protection of personal information aims to preserve the confidentiality and security of individuals' personal information. In the digital age, every action we take online leaves a trail of personal information, whether it's using a credit card or GPS, or interacting on social networks. This data is valuable to companies, which engage in what researcher Shoshana Zubov calls «surveillance capitalism,» and to governments that may monitor certain individuals for national security reasons.

The definition of personal information is very broad, encompassing any information that directly or indirectly identifies a person. Some of this information is considered sensitive due to its nature or the context in which it is used. For example, financial information, sexual orientation, political affiliation, health, etc. The management of this data generally requires the explicit consent of the individuals involved to ensure increased transparency.

Privacy protection aims to give citizens control over their personal information. This includes the right to be informed about the use of their data, to freely consent to this use, and to ensure that the data is used in accordance with the announced purposes.

Ultimately, digital trust is closely related to the protection of personal information. It represents the trust that individuals place in companies regarding their ability and willingness to respect their consent and protect their personal information. When a company or organization is transparent in its data collection and use practices, respects the rights of individuals, and implements adequate security measures, it contributes to strengthening digital trust.

02 How is the regulation of personal information protection evolving?

In Canada, the protection of personal information in the private sector is mainly governed by the Personal Information Protection and Electronic Documents Act (PIPEDA). However, there have been recent developments aimed at modernizing and strengthening the regulation of personal information protection.

Bill C-27, also known as the Consumer Privacy Protection Act (CPPA), aims to enhance individuals' control over their personal information, require more transparency from companies, and introduce stricter penalties for privacy violations. The bill was introduced in November 2020 and is currently under review.

At the federal public sector level, the 1985 Privacy Act applies, and the government is conducting consultations to potentially reform it.

In Quebec, legislation for both private and public sectors has been reformed by Bill 64, adopted in September 2021 and becoming Law 25. This law positioned Quebec as a leader in personal information protection by establishing rigorous standards comparable to the European Union's General Data Protection Regulation (GDPR). It strengthens the oversight powers of the Access to Information Commission (CAI) and introduces dissuasive financial penalties.

03 Why is the management of personal information essential for a company or organization today?

Trust in data, which encompasses privacy protection, security, and data governance, has become a major strategic issue for organizations, going beyond regulatory obligations. While laws like the GDPR or Law 25 encourage compliance through significant sanctions (e.g., 5% of revenue or $20 million), their true importance lies in their role as catalysts for organizational resilience and risk management, particularly in the face of ransomware or geopolitical crises.

In a context where data breaches are inevitable, the challenge is to ensure business continuity while avoiding violations that can have serious consequences for both companies and individuals. Furthermore, the emergence of generative AI illustrates how reliable and well-governed data is essential. Without them, innovative technologies can produce erroneous results, as demonstrated by a recent Canadian case where a chatbot hallucinated a discount that a company had to honour.

Finally, data, especially personal information, are now at the core of most business models. Reliable information is essential for innovation, understanding customer needs, and adapting to markets. In this sense, a well-designed personal information protection program can become a lever for establishing robust data governance and protection. I think of one of my clients who has successfully created an integrated digital trust program and achieved significant economies of scale by aligning their teams, processes, and technologies. Investing in trustworthy data pays off.

04 How does the implementation of a personal information protection program take place, and what role does internal audit play?

Achieving compliance or creating a personal information protection program is a complex process. There are two main steps: defining a governance structure and implementing programs to transparently inform users, respect their consent and other rights such as access rights, and responsibly manage the data lifecycle. All of this contributes to establishing digital trust.

Regarding the definition of a governance structure, the first step is to appoint a privacy officer acting under the delegation of the company's leader, who is personally accountable under the law. Then, multidisciplinary committees are formed, bringing together operations, IT, cybersecurity, data governance, and risk management stakeholders. These committees work together to define the company's privacy policy by translating legal requirements into business requirements.

The central governance challenge in personal information protection lies in establishing a robust first line of defense. This involves ensuring that operational resources handling personal information on a daily basis (Line 1A) have a clear understanding of the requirements and practices to adopt. It is equally essential that their supervisors (Line 1B) share this understanding and play an active role in supervision and awareness.

With a well-trained and engaged first line, the privacy office (Line 2) can focus on its coordination, control, and steering functions while delegating some controls to other key functions such as internal control or risk management.

The internal audit function (Line 3) possesses the expertise and occupies a privileged position to conduct governance reviews. It is able to ask key questions such as: Are roles and responsibilities clearly defined? Do committees have adequate charters? Do supervisory personnel have access to the right information in a timely manner to make the right decisions? Is the implemented strategy aligned with the objectives set by the governance structure? Have risks been identified, reported, and is the monitoring process robust enough to ensure that risk mitigation measures are implemented? etc.

05 Once the governance structure is established, how is data lifecycle management established? What role can internal audit play in data lifecycle management?

The compliance process continues with an assessment, which can be conducted by internal audit or other actors, to evaluate compliance with legal requirements. This helps identify gaps and design a remediation program.

The company then needs to understand how it uses personal information («processing») and its level of compliance. To do this, it conducts a mapping of its processing activities (also known as an «inventory» or «register»). This mapping can be obtained through interviews and technical analyses to trace the data lifecycle across different layers of the architecture (processes, applications, infrastructures). Once the inventory is established and gaps are identified, the company can base its prioritization decisions on reliable data and track its progress accurately.

Key processes, such as consent management, individual rights, or privacy by design, are then defined and implemented. To industrialize them, many companies adopt specialized tools (Privacy Enhancing Technologies) that automate certain tasks and facilitate documentation and information sharing. Special attention is given to raising awareness and providing training to all employees, as data protection is a collective responsibility.

Internal audit can intervene to ensure that the company maintains its level of compliance over time. Through recurring audits, it assesses both organizational aspects (application of processes, documentation, leadership) and technical aspects (scans and controls of environments). These audits help establish robust and sustainable programs, avoiding superficial compliance limited to theoretical policies and processes.

06 What are some of the key controls that an internal auditor should observe during an audit?

Each organization should define its key controls, but generally, the maturity level of an organization can be estimated by checking the existence of roles or committees dedicated to privacy, their influence with top management, the presence of a privacy program, an inventory of processing activities, a privacy by design approach for new projects, as well as processes such as consent management, individual rights, data deletion after the retention period, incident management, and most importantly, the practical application of these processes.

07 What advice would you give to internal auditors to stay informed about the subject of personal information protection?

I highly recommend that internal audit teams ensure that at least one member is trained in privacy matters, which can be achieved through CIPM or CIPP training offered by the IAPP. These trainings provide a deep understanding of the operationalization of privacy, with CIPM focusing on the operational aspect while CIPP addresses regulatory issues. Additionally, the website of the Commission d'Accès à l'Information (CAI - Access to Information Commission) offers valuable resources, as the CAI is the entity responsible for interpreting and applying the law in Québec.

The Knowledge Network Montreal chapter of the IAPP organizes bi-monthly conferences on privacy-related topics, and I strongly encourage you to participate as non-members are welcome to these events. Furthermore, the websites of different regulators (provincial, federal, European, etc.) have excellent online newsrooms where you can find all the important news. The IAPP website also offers a high-quality virtual newsroom where you can stay informed about the latest developments in the field of privacy.

The Montreal chapter of IAIM also offers training on this subject.

08 Finally, how do you perceive the future of personal information management?

I believe that privacy management will become an integral component of everyday business operations, similar to what happened in Europe about three years after the GDPR came into effect.

The emerging role of privacy engineers is particularly crucial, as these IT professionals are capable of identifying technical solutions to ensure privacy compliance and seamlessly integrate it into the user experience and the company's project lifecycle.

Furthermore, the advent of AI presents fascinating challenges in terms of privacy protection, especially regarding algorithms that can act as «black boxes.» It is essential to be able to explain and control the use of personal information by these systems to provide transparent information, manage consent, and individual rights.

Interview conducted by
Maelle Gillet for the Institute of
Internal Auditors – Montreal Chapter

About IAPP

The IAPP (International Association of Privacy Professionals) is the largest and most comprehensive global information privacy community and resource, helping practitioners develop and advance their careers, and organizations manage and protect their data. Starting in 2000 with only a handful of dedicated privacy pros and just 2 corporate members, the organization has grown to over 75,000 members across 100+ countries.

IAPP has become the recognized leader in the privacy industry, facilitating conversations/debates and collaboration among key industry leaders and organizations.

About IAI Montréal

Founded in March 1945, the Institute of Internal Auditors, Montreal Chapter (IAI Montréal), is a non-profit organization incorporated under the Quebec Companies Act. It brings together nearly 900 members and is governed by a board of directors supported by committees.

Our chapter's mission is to support and develop internal audit professionals throughout their careers, as well as promote the role and value of the profession. Our vision is to be recognized as a preferred partner by the business community, ensuring relevance and innovation within the profession.

Our slogan? The ultimate partner for the growth of our members!

IAI
Canada
Montréal