THE VITAL ROLE OF COOPERATION IN ACHIEVING DATA PRIVACY COMPLIANCE

Erin Schachter LL.M. Therrien Couture Joli-Coeur

In today's digitally interconnected world, data privacy has emerged as a paramount concern for businesses operating across various sectors. With the proliferation of technology, data flows seamlessly across borders, subjecting businesses to a myriad of privacy laws and regulations. To navigate this complex landscape successfully, organizations must prioritize compliance with data privacy requirements.

The term "compliance" in the realm of privacy encompasses an organization's commitment to upholding privacy obligations within its jurisdiction and beyond, wherever data is collected. This entails adhering to a range of legal mandates, including notifying authorities of cybersecurity incidents, establishing internal data handling processes, publishing privacy policies, and appointing privacy officers. As legislative frameworks evolve globally, adherence to these standards becomes increasingly crucial.

With the use of so many third-party services, it is nearly impossible to contain the flow of data within one jurisdiction. This means that businesses must be conscious of data privacy obligations within their own jurisdiction and abroad in the event they are collecting data from other states or countries. For example, if a business collects data from individuals in Europe or Canada, it will be subject to legislation in those jurisdictions. For this reason, it has never been more important to take a mindful approach to data privacy.

While many businesses take initial steps toward compliance, such as appointing a privacy officer or implementing cybersecurity measures, they often encounter challenges in sustaining these efforts. This stagnation underscores the importance of fostering cooperation within organizations as a fundamental precursor to achieving compliance. Regardless of the number of policies in place, effective compliance hinges on seamless communication and collaboration among diverse departments, including human resources, finance, IT, and legal. It's important to note that while this article primarily focuses on internal cooperation, external collaboration with government entities, suppliers, subcontractors, and business partners is equally vital.

Illustrating the ramifications of departmental silos, consider the following scenarios where a lack of cooperation impedes compliance efforts:

SCENARIO 1: HIRING PROCESS OVERSIGHT

Your organization wants to hire a new resource. It publishes a job advertisement and collects the CVs of several candidates. The position is filled, and a candidate starts working for the organization. So far, the human resources department and the IT department have not considered issues related to the protection of personal information, and the privacy officer has not been involved in the hiring process. What problems could arise?

1. Data Collection Issues: The human resources department may inadvertently collect data without appropriate consent, violating privacy regulations.
2. Retention Period Violations: Data retention practices may contravene jurisdictional laws, leading to legal liabilities.
3. Inadequate Data Security: Data storage practices may lack necessary security measures, exposing sensitive information to breaches.
4. Lack of Employee Training: Newly hired employees may not be adequately trained in internal privacy policies, increasing the risk of inadvertent data mishandling.

SCENARIO 2: DEPARTURE OVERSIGHT

An employee decides to leave the organization where he worked for four years to join a competitor. He discovers that he

still has access to his former employer's systems and decides to use old files for the purposes of his new job. In this scenario, human resources and IT did not communicate with the privacy officer, and the organization did not implement appropriate measures to ensure the protection of personal and confidential information held by the organization. Personal information was, therefore, accessed without authorization, potentially constituting a privacy incident under certain laws that should be reported to the appropriate authorities.

SCENARIO 3: INCIDENT RESPONSE OVERSIGHT

Your organization experienced a privacy incident. It believes it should notify the affected individuals due to requirements in that jurisdiction and is considering issuing a press release. A journalist calls your organization, and one of the staff members responds to the information request without consulting the privacy officer. Incorrect information is provided, which must then be retracted, tarnishing the company's reputation. Communication errors can seriously impact the effectiveness of incident response plans, emphasizing the importance of training staff on proper procedures and involving all relevant stakeholders, including the privacy officer.

To address these challenges effectively, organizations must prioritize three key initiatives:

1. Establishing Clear Roles:

Designate a privacy officer and key personnel within each department responsible for assisting the privacy officer. This ensures accountability and oversight across the organization. We have provided below some suggestions on how to establish these roles.

- Establish a list of departments within your organization and the individual who leads that department.
- Determine hierarchy: who within the department is best placed to be a member of an internal privacy committee. It may be the head of the department or another individual. However, you will want to choose someone with authority and who will be involved in major decision-making. For example, if you have a human resources department, you may want to involve the head of human resources as they will be aware of every new hire and termination of employment.
- Create a committee with the members of each of these departments and ensure they are trained in internal privacy compliance. They will need to be aware of all internal policies, have a good basic understanding of privacy law basics and to whom they should address any questions or concerns.
- Train committee members. The reality is that today, many individuals unknowingly use personal data in their day-to-day work. Training individuals on the basics of privacy and even signing up committee members for a course can be an excellent way to prepare members for their roles. We discuss training in greater detail below.
- Check in with the committee. There should be periodic check-ins with the members of any committee to update internal policies, discuss what is working and what is not working, and ensure that any issues are handled.
- Update roles as needed. If there is any change in leadership, it will be necessary to ensure individuals filling a new role are onboarded appropriately in matters of data privacy and understand their role.

The advantage of creating this team and naming the right individuals is that it both ensures cooperation between departments, which helps with compliance, and it helps relieve some pressure from the privacy officer. There is an enormous amount of work required to maintain security for personal information, and this task becomes much easier if the privacy officer is not chasing down information.

2. Implementing Concrete Checklists & Policies:

Develop comprehensive checklists for key moments such as hiring, termination, data incidents, and technology acquisitions involving personal information. These checklists serve as practical guides to ensure compliance at every stage of operation.

We have provided a guide that serves as an example of a checklist for a human resources department. You can modify the guide to suit the practices of your organization. The idea is that you will create a checklist to ensure that each department understands the steps they must take to protect privacy and at which moment they should involve the privacy officer. If we return to the scenarios we provided above and if human resources has a checklist to onboard any new employee, they will be better placed to confirm:

- That the individual has consented to the use of their personal information.
- The employee is trained on privacy matters and understands their duty towards other employees and clients in protecting data.
- The employee will use any device they are provided, such as a phone or a computer, in a safe manner.
- Their access is managed to ensure they only have access to files that are necessary for their work.

In the event that their employment is terminated, another checklist can be used to ensure that any access they were granted is revoked and all devices are returned. Policies can be used to ensure that a structure is in place to govern all privacy matters.

The privacy officer can revisit these checklists annually and make the necessary changes. Privacy is an ever-evolving landscape for every business, and by having clear checklists, internal policies, and cooperation between departments, a business can continue to evolve its privacy practices with its reality.

3. Enforcing Robust Training Programs:

Implement ongoing training programs to keep employees abreast of privacy policies and procedures. Open lines of communication must be maintained to facilitate cross-departmental collaboration and adherence to privacy protocols.

The final step in ensuring cooperation and compliance is proper training. There should be more extensive training for individuals in a situation of authority who will be part of the privacy committee. Employees who are not on the privacy committee should equally be trained. Both existing and new employees should frequently have updates to their data privacy training as new practices emerge.

In conclusion, while achieving compliance with data privacy regulations may seem daunting, collaboration and cooperation among departments are indispensable in navigating this complex landscape. By prioritizing internal cooperation and fostering a culture of proactive compliance, businesses can safeguard the privacy of both customers and employees, thereby mitigating legal risks and upholding trust in an increasingly data-driven world.

Erin Schachter, LL.M., is a lawyer specializing in intellectual property law, technology law, and data privacy, with a focus on international law. Fluent in both English and French, she frequently attends USLAW conferences and contributes to content on data privacy. Erin excels in advising clients on privacy laws in Canada.