Issue #2 June 18, 2015

Privacy Programs

by *Lyndsay A. Wasser*, CIPP/C, Co-Chair Privacy

In our first Privacy Basics bulletin, we described the importance of ensuring that your organization has useful, comprehensive privacy policies. However, policies are only one component of a successful privacy compliance strategy. Too often, organizations spend time and money developing good privacy policies, but do not take the next step of implementing the policies and ensuring that the organization has an appropriate infrastructure to support compliance with such policies.

A comprehensive privacy program includes, at a minimum, the following elements:

1. Appointment of a privacy officer (or for larger organizations, a privacy team)

Some privacy statutes explicitly require appointment of a person who is responsible for the organization's compliance with the legislation.[1] Even where this requirement is not explicit, appointment of one or more privacy officers is typically considered to be an implied obligation pursuant to statutory accountability obligations. In order for the privacy officer to be effective, such person should have access to and influence with senior management and other decision makers.

2. Privacy audits

It is impossible to adequately protect personal information without understanding the flow of information through and within the organization. At a minimum, it is crucial for the organization to assess: (i) what personal information it collects, and how such information is

[1] For example, the *Personal Information Protection and Electronic Documents Act*, the *Personal Information Protection Act* (Alberta) and the *Personal Information Protection Act* (British Columbia).

collected; (ii) where information is stored, and what security measures are used to protect the information; (iii) the sensitivity of the information that the organization collects and stores; (iv) who has access to the information and for what purposes; (v) the purposes for which the personal information is used; and (vi) the circumstances surrounding any disclosure(s) of personal information, including data protection provisions in contracts with third parties.

To obtain a copy of McMillan's comprehensive Privacy Audit Checklist, please contact your McMillan advisor.

3. Privacy training for employees

The majority of privacy breaches are caused by human error. Often these errors are made by employees who do not understand applicable privacy laws, the organization's privacy policies and/or their obligations under such laws and policies. Therefore, privacy training is crucial for compliance with privacy laws and for breach prevention.

4. Privacy policies

Privacy policies were addressed in detail in Issue #1 of McMillan's Privacy Basics series. To view Issue #1, click *here*.

5. Confidentiality agreements

Privacy training and policies are useful tools, but binding contractual obligations are always better. Since employers can be held vicariously liable for privacy breaches caused by employees, organizations should require that employees sign confidentiality agreements before providing them with access to personal information (especially sensitive information).

6. Outsourcing controls/Data protection agreements

When organizations outsource or subcontract functions to third parties, they are generally still responsible for the protection of personal information that is processed in connection with such functions. Therefore, organizations should review the privacy practices and policies of their service providers, and also ensure that they enter into data protection agreements with such third parties. Alternatively, data protection and privacy provisions can be included directly in the service agreement itself.

7. Procedures for responding to complaints, inquiries and access requests

Privacy legislation in a number of jurisdictions contains specific requirements applicable to complaints, inquiries and/or access requests. Often there are time limits for organizations to respond to these communications. Contact information for the person(s) who can respond to complaints, inquiries and access requests should be available to individuals whose personal information is handled by the organization. Also, employees should be able to identify a communication that requires a response under applicable privacy legislation, and they should understand how and where to direct such inquiries, complaints and requests.

8. Breach response plan

Privacy breaches can occur despite an organization's best efforts to prevent them. When such incidents occur, it is important to have a response plan in place so that valuable time is not lost scrambling to assign roles and responsibilities. At a minimum, every breach response plan should involve steps to: (i) contain the breach, (ii) evaluate risks, (iii) notify relevant parties in accordance with applicable laws and contractual obligations, and (iv) prevent future incidents.

9. Privacy impact assessments ("PIA")

When an organization begins planning any new program or initiative that will involve collection, use or disclosure of personal information, it should consider conducting a PIA at an early stage. This will allow the organization to identify legal requirements, assess potential risks, and develop solutions to mitigate such risks. Building privacy compliance into the plan or proposal from the outset will avoid the wasted time and resources involved in developing projects that are later determined to be offside of privacy law requirements. For an example of how inadequate privacy controls can have disappointing consequences, see McMillan's client bulletin *Bell Gets a Bad Rap for its RAP (Relevant Advertising Program)*.

10. Regular review and updates of policies and training

Privacy law is currently in a period of rapid development. Furthermore, organizations are rarely static. In order to ensure that privacy policies reflect recent legal developments and

changes to the way that organizations collect, use and disclose personal information, privacy policies should be periodically reviewed and updated. When such changes occur, employees should receive training on any new requirements or restrictions. Ideally, training updates would also include a refresher on important basics, as it is important for employees to be reminded of their core obligations from time-to-time.

For more information on many of these topics, stay tuned for upcoming Privacy Basics bulletins. You can also contact your McMillan advisor at any time for more information on these topics and/or a copy of our standard Privacy Program Checklist, Privacy Audit Checklist, or Breach Response Checklist.

For more information on this topic please contact:

Toronto Lyndsay A. Wasser 416.865.7083 lyndsay.wasser@mcmillan.ca

a cautionary note