2022 Privacy risk management – Top tips for organizations

10 mai 2022

Changing laws and privacy culture around the world, a growing sophistication of cybersecurity threats, innovations in response to the COVID-19 pandemic and environmental, social and governance priorities, increased data outsourcing and a peak in M&A deal activity means that privacy issues are more prevalent than ever.

Organizations know that the consequences of failing to safeguard personal information in the face of an incident can be enormous. What steps should they prioritize to mitigate risks and mature their privacy management programs?

This article identifies our five top tips and a checklist to get you started.

1. Respond, don ’t react: Accountability and governance

We are seeing a significant trend towards development and reform of privacy laws across Canada and globally. In Canada, modernization of privacy laws has generally involved enhanced transparency of organizations’ practices, increased consumer control of personal information, addressing new/emerging technology issues (such as pseudonymized and anonymized information, automated decision-making and biometrics) and bolstered enforcement powers of privacy commissioners. See BLG's previous articles Changes to B.C.'s public sector privacy legislation, Special committee recommendations to modernize B.C.’s private sector privacy law and Québec Privacy Law Reform: A Compliance Guide for Organizations for more information.

Organizations should take steps to mature their privacy management programs to comply with – or to prepare to comply with – modernized privacy laws, rather than reacting to changes.

Checklist

Directors and senior management

☐ Prepare directors and senior management for potential legislative changes, potential impacts of those changes and resourcing challenges.

Policies and procedures

☐ Conduct an inventory of the policies and procedures in place to protect personal information throughout its life cycle.

☐ Identify and consider the approach in addressing any gaps in the policies and procedures.

☐ Confirm that the organization has a platform to share its policies and procedures on its internal and external websites (as applicable).

Employee training

☐ Confirm that the organization has a training program for employees who handle or have access to personal information.

Data mapping

☐ Conduct a data mapping exercise to document the organization's personal information and its management practices – this is the foundation to any program! External legal counsel can support a data mapping exercise by providing departmental surveys.

☐ Prepare inventories of technological products or services offered internally or externally that collect personal information. Also prepare inventories of consent forms or other documents used to obtain consent from individuals with respect to their personal information.

☐ Confirm that the organization's personal information, management practices and inventories are classified under its document management protocols.

Data minimization and retention

☐ Confirm that the organization is not collecting more personal information than it needs.

☐ Confirm that the organization is not retaining personal information for too long.

Other departments

☐ Involve and leverage departments other than just legal (such as IT/security, human resources, procurement and operations) to enhance organizational accountability as a whole.

Checklist

Incident response team

☐ Define clear roles and responsibilities for incident response internally (including communications and other departments) and externally (including managed security service providers, forensics consultants, public relations advisors, external legal counsel and insurance providers) and keep a contact list of those involved (including back ups).

☐ Engage external firms and service providers now, so that they are prepared in the face of a cybersecurity incident. Involve and coordinate with the insurance provider during this process, as the insurance provider might only work with select firms and service providers.

☐ Develop a legal privilege and legal compliance strategy. Working with external legal counsel as a cyber coach, rather than other types of experts, will preserve solicitor-client privilege and litigation privilege and ensure organizational legal compliance when responding to a cybersecurity incident. See BLG's previous article Cybersecurity incident response – Tips from the trenches.

☐ Define communication channels internally and externally and prepare a communication plan if the organization's business email service or other usual communication channels are compromised by a cybersecurity incident.

☐ Form a cyber/privacy committee of cross-departmental teams (including the privacy officer and IT/security) that meets routinely to create understanding, open dialogue and identify risks and solutions.

☐ Identify where the organization keeps logs or records of any incidents.

Testing and refining

☐ Test the incident response plan to reduce the risk of errors and streamline the response in the face of an actual cybersecurity incident. A tabletop exercise can help identify inefficiencies and impracticalities in the incident response plan.

☐ Refine the incident response plan to address the inefficiencies and impracticalities identified during testing.

Cyber insurance

☐ Understand the organization's cyber insurance, including the insurance provider, the policy (*e.g.,* limits, coverage amounts and the expiry date), the requirements for notification and incident response decisions and the associated expenses.

☐ Avoid invalidating cyber insurance coverage by failing to follow the insurance provider's requirements. For example, in a ransomware attack, the insurance provider will likely require specific steps to be taken prior to the consideration of payment of any ransom fee.

☐ Engage external legal counsel to provide cyber hygiene insurability audits and thus streamline the insurance application and reduce costs. See BLG's previous article Cyber hygiene checklist: Tick these boxes to lower your cybersecurity risk and insurance costs.

Cyber risk mitigation

☐ Take ownership of cybersecurity risk mitigation by implementing the data minimization principle, training employees to identify cybersecurity threats, assessing cybersecurity policies and procedures (such as BYOD policies and procedures) and managing risks of outsourcing.

Checklist

Data minimization

☐ Apply the data minimization principle to innovative technology. If the personal information is not needed, do not collect it (even if the technology can collect it).

☐ Consider eliminating the use of personal information by artificial intelligence technologies.

☐ If the organization has determined that it is reasonable to check vaccination information of employees, do not store the actual vaccination information, but rather only capture whether or not the employees have complied with the organization's internal vaccination policy.

Ethics perspective

☐ Incorporate an ethics perspective when creating or procuring innovative technology that collects personal information.

☐ Consider if there is a potential for biased or discriminatory impact or application of the data that has been collected, if there is any potential for inadvertent surveillance or if there are safety and other societal implications (*e.g.*, the innovative technology being perceived as taking the jobs of the organization's workforce).

Remote work

☐ Educate employees about the risks of remote work and organizational policies and procedures with respect to remote work (such as preferred video-conferencing platforms and when to log onto a VPN).

Privacy by design and privacy impact assessment

☐ When creating innovative technology, guide the organization through privacy by design principles (such as consent, safeguards and accountability).

☐ Consider having a privacy impact assessment template.

Checklist

Due diligence

☐ Assess the potential risks and benefits of outsourcing.

☐ Consider appropriateness of using a proposed service provider for the required service and understand the purpose for engagement.

☐ Assess the types of personal information transferred to the service provider.

☐ Understand the service provider's privacy and security practices. Review the service provider's privacy policy and terms of service and confirm that the service provider has implemented appropriate policies and procedures.

☐ Conduct due diligence on the proposed service provider. Consider experience and ability to provide the service, business reputation, financial strength and any past issues, complaints or litigation.

☐ Identify any jurisdictional issues based on where the service provider is located.

Contract

☐ Use the contract to protect the organization and include (as appropriate) provisions that address the protection of personal information, permitted and prohibited uses of personal information, the return or destruction of personal information at the termination of the contract, a requirement of the service provider to promptly notify the organization of any breach or attempted breach of confidentiality obligations, audit rights (*i.e.*, the right for the organization to request documents and to carry out audits to verify the service provider's compliance with its contractual obligations) and other key issues (*e.g.*, subcontractors, organizational control, insurance, indemnities and exclusions from limitation of liability clauses).

☐ Prepare a template contract or set of clauses that address the processing of personal information. If the organization cannot control the paper, use internal policy (minimum standards) or regulatory guidance as leverage.

Ongoing monitoring

☐ Implement policies and procedures for regular, ongoing monitoring of the service provider.

☐ Review any terms and conditions that have changed.

☐ Assess material changes to the service provider relationship.

Other practical considerations

☐ Review and update the organization's privacy policy to reflect the use of service providers.

☐ Limit service provider access to personal information.

☐ Implement data sharing procedures for providing personal information to service providers.

☐ Consider if additional consent is required with respect to outsourcing.

☐ Implement and regularly update the organization's incident management framework.

☐ Monitor developments on Canadian personal information protection laws, including those on outsourcing to service providers.

Checklist

Due diligence

☐ Engage in privacy and cyber-specific due diligence of the target.

☐ Understand the target's collection and use of personal information, including the data flow through the target's organization.

☐ Understand the privacy laws that apply to the target's personal information handling practices and consider whether the target has complied with specific obligations under those privacy laws.

Purchase agreement

☐ Ensure the purchase agreement addresses privacy and cyber risks identified in due diligence, including appropriate representations and warranties.

☐ Include indemnities, holdbacks and insurance obligations that address privacy and cyber risks (where appropriate).

☐ Ensure the purchase agreement contains appropriate provisions that comply with applicable privacy laws to permit the sharing of personal information post-closing.

Post-closing

☐ Implement policies and procedures to transfer personal information to the purchaser post-closing.

☐ Notify individuals of the disclosure of their personal information during the M&A transaction process as required by applicable privacy laws.

☐ Remediate the privacy and cyber risks identified in due diligence.

Par

Sepideh Alavi, Katherine M. Stanger, Danielle Windt

Services

Droit des sociétés et droit commercial, Fusions et acquisitions, Franchisage et distribution, Cybersécurité, respect de la vie privée et protection des renseignements personnels, Vente en ligne et commerce électronique, Commerce de détail et tourisme d'accueil

---

BLG | Vos avocats au Canada

Borden Ladner Gervais S.E.N.C.R.L., S.R.L. (BLG) est le plus grand cabinet d'avocats canadien véritablement multiservices. À ce titre, il offre des conseils juridiques pratiques à des clients d'ici et d'ailleurs dans plus de domaines et de secteurs que tout autre cabinet canadien. Comptant plus de 725 avocats, agents de propriété intellectuelle et autres professionnels, BLG répond aux besoins juridiques d'entreprises et d'institutions au pays comme à l'étranger pour ce qui touche les fusions et acquisitions, les marchés financiers, les différends et le financement ou encore l'enregistrement de brevets et de marques de commerce.

blg.com

Bureaux BLG

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000, rue De La Gauchetière Ouest
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749