THE TOP 5 THINGS YOU PROBABLY ARE NOT DOING (BUT SHOULD BE DOING) TO COMPLY WITH CANADIAN PRIVACY LAWS: *ISSUE #3: MANAGING VENDORS*

Posted on September 3, 2024

Categories: Insights, Publications

Under Canadian privacy laws, organizations that transfer personal information ("**PI**") about customers, employees or other parties to a third party vendor for processing remain responsible for the protection of that PI.

For example, the federal *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") requires an organization to use contractual or other means to provide a comparable level of protection while PI is being processed by a third party. Similarly, private sector privacy legislation in Alberta and British Columbia, as well as provincial public and health sector privacy laws, provide that organizations remain accountable for PI that is processed by service providers.

Quebec's *Act respecting the protection of personal information in the private sector* (the "**Quebec Act**") allows a person carrying on an enterprise to communicate PI to a third party without an individual's consent if the PI is necessary for carrying out a mandate or performing a contract of enterprise or for services. However, the person carrying on the enterprise must enter into a written contract with the third party including measures the third party must take to protect the confidentiality of the PI, to ensure that the PI is used only for carrying out the mandate or performing the contract, and to ensure that the third party does not keep the PI after the expiry of the mandate or contract.

The Quebec Act also requires that a person carrying on an enterprise conduct a privacy impact assessment ("**PIA**") prior to entrusting a person or body outside Quebec with collecting, using, communicating or keeping PI on the enterprise's behalf. The written agreement between the parties (as mentioned above) must include terms to mitigate any risks identified in the PIA. For more information about conducting PIAs, see our earlier issue here.

Mishandling of PI by a vendor can expose an organization to significant risks, including privacy complaints, investigations by regulators, fines and/or litigation, in addition to potential impacts on the organization's reputation and relationships with its customers, employees and business partners. For example, if a vendor

experiences a data breach impacting PI that is controlled by your organization, your organization may be required to report the incident to privacy regulators, notify impacted individuals, take steps to mitigate potential harm to individuals, and even incur costly legal fees in connection with responding to regulatory investigations and/or claims.

Protecting PI that is processed by vendors requires a multi-pronged approach, including:

- Conducting thorough due diligence to understand the vendor's privacy policies and practices and cybersecurity posture, and whether the vendor has experienced any historical data breaches, privacy complaints, investigations, claims or other disputes;
- Entering into appropriate contractual terms with vendors, including all terms required by applicable statutes and recommended in relevant regulatory guidance (see, for example, the federal privacy regulator's guidance on the contents of written contracts with vendors in PIPEDA Findings #2019-001);
- Monitoring and, where appropriate, periodically auditing vendors to ensure compliance with applicable privacy and data protection laws and contractual terms; and
- Ensuring that vendors return or securely destroy PI when it is no longer needed to provide the vendor's services.

If you are a vendor offering your services to Canadian businesses, it is equally important to confirm that your contracts with your customers reflect applicable Canadian privacy laws and regulatory guidance, appropriately allocate responsibility and risk for data breaches, obtaining valid consent, managing data subject rights requests and other privacy and data protection matters, and do not contain cybersecurity or other commitments which your organization cannot uphold. You should also ensure that your privacy and cybersecurity policies and procedures can withstand scrutiny by potential customers, and, in particular, reflect the specific requirements of Canadian privacy laws.

Action Items

Effectively managing vendors who process PI on behalf of your organization requires the following proactive measures: (1) developing a standard questionnaire or checklist to vet the privacy and data security practices of potential vendors and their products/services; (2) developing internal policies and procedures regarding the engagement of vendors who process PI; (3) drafting a template data protection addendum and/or set of privacy and data protection provisions that can be included in agreements with vendors; (4) considering the sufficiency of contractual terms with existing vendors, including to account for recent statutory changes and regulatory guidance; (5) prior to engaging a vendor, conducting any PIAs that are required by applicable laws or by your internal policies and procedures; (6) developing a structured program for monitoring vendors'

compliance with applicable laws and their contractual obligations; (7) training employees about your organization's processes for vetting and monitoring vendors; and (8) ensuring that your organization's privacy policies, notices and consent language accurately describe how vendors process PI on your organization's behalf.

If you are a vendor offering your services to Canadian businesses, your organization should: (1) develop a template data protection agreement and/or set of privacy provisions that can be included in agreements with customers for whom your organization processes PI; (2) develop and maintain a system for tracking compliance with your contractual commitments regarding privacy and cybersecurity; and (3) ensure that your privacy compliance program takes into account Canadian privacy laws and regulatory guidance, as well as cybersecurity best practices, so that you are prepared to respond to customers' due diligence inquiries.

McMillan's Privacy and Data Protection team can help your organization to implement the action items outlined above. Contact your McMillan representative to obtain the support your organization needs to ensure compliance with this critical privacy compliance issue.

by Lyndsay A. Wasser and Kristen Pennington

A Cautionary Note