Bulletin | Cybersecurity, Privacy and Data Protection

February 2021

Privacy Commissioner reports provide guidance for outsourcing agreements

Canadian private sector privacy laws generally permit organizations to engage service providers to process personal information for the organizations. Organizations remain accountable for the personal information they transfer to a service provider, and must use contractual and other safeguarding measures to protect the personal information while in a service provider's custody. In 2020, the Privacy Commissioner of Canada issued two investigation reports that provide guidance regarding measures to help ensure that outsourcing arrangements comply with private sector privacy laws. All organizations that engage service providers to process personal information can benefit from the guidance.

Fundamental principles

Canadian private sector privacy laws – the Canadian *Personal Information Protection and Electronic Documents Act* (PIPEDA) and substantially similar laws in Alberta, British Columbia and Québec – regulate the collection, use, disclosure and retention of personal information by private sector organizations in the course of commercial activities in Canada. Those laws are based on internationally recognized *Fair Information Principles*, including the principles of Accountability and Safeguards.

- The Accountability principle provides that an organization is responsible for personal information in its possession or under its control, including information the organization has transferred to a third party (e.g., an outsourced service provider) for processing. An organization must use contractual or other means to provide a comparable level of protection while personal information is being processed by a third party, and implement policies and practices for compliance with privacy laws.
- The Safeguards principle requires that an organization protect personal information using security safeguards appropriate to the sensitivity of the information. The safeguards should include physical, organizational and technological measures to protect personal information against loss or theft, and unauthorized access, disclosure, copying, use, or modification.

PIPEDA and the Alberta *Personal Information Protection Act* also impose personal information security breach reporting, notification and record-keeping obligations on an organization that suffers a breach of security safeguards involving personal information under the organization's control, including information transferred to an outsourced service provider for processing.

Canadian private sector privacy laws are principles-based statutes. For the most part, they set out broadly stated rules or principles, rather than detailed prescriptive restrictions and requirements. While that approach has benefits (e.g., flexibility and efficiency), it also can result in uncertainty. Consequently, privacy commissioner guidance is an important source of insight regarding minimum requirements for legal compliance.

Canadian privacy commissioners have issued guidance to help organizations comply with privacy laws applicable to outsourcing arrangements (including arrangements with related companies) that involve the processing of personal information. For example, see *Privacy and outsourcing for businesses*, *Guidelines for processing personal data across borders*, *What you need to know about mandatory reporting of breaches of security safeguards*, and Investigation Reports #2019-001 and #2019-003.

Privacy Commissioner investigation reports

In 2020, the Privacy Commissioner of Canada issued two investigation reports that provide guidance regarding outsourcing arrangements involving the processing of sensitive personal information.

Report of Findings #2020-001 – Financial Institution Fraud Claims Processing

The Privacy Commissioner of Canada investigated a financial institution's outsourcing of aspects of its fraud claims processing to a service provider in India. The investigation resulted from a complaint by a former employee of the financial institution. The service provider had access to large amounts of sensitive personal information about the financial institution's customers. The Privacy Commissioner's Report concluded that the financial institution had satisfied its accountability obligations because the financial institution ensured a comparable level of protection for the information through a robust contract and other methods, including regular audits to ensure compliance with contractual requirements.

The Report provides the following general guidance regarding transfers of personal information to service providers:

- For purposes of compliance with PIPEDA, personal information is "transferred" to a service provider when the personal information is accessed and processed by the service provider, even if the service provider does not store the personal information.
- An organization's contract with a service provider is the primary means by which the organization protects personal information transferred to the service provider.
- A robust contract is especially important if a service provider is in a foreign jurisdiction.
- A contractual requirement that a service provider comply with Canadian privacy laws is not, on its own, sufficient to ensure an adequate level of protection to personal information transferred to the service provider.
- A contract with a service provider should address all PIPEDA restrictions and requirements applicable to the particular arrangement.

The Report notes some of the contractual, physical, organizational and technological measures used by the financial institution to safeguard personal information transferred to the service provider:

- **Limited access:** The service provider had only remote access to a limited amount of personal information through a portal managed by the financial institution. The personal information remained stored by the financial institution in Canada.
- **Limited permissible use:** The contract prohibited, and associated safeguards prevented, the service provider from accessing, using or disclosing personal information for any purpose other than those set out in the contract, and from retaining any personal information in India.
- **Risk assessment:** Before entering into the outsourcing arrangement, the financial institution performed a detailed risk assessment to identify and mitigate potential privacy risks, and incorporated the risk assessment findings into the outsourcing contract.
- **Employee background assessment:** The service provider was contractually required to conduct background verification and annual reverification for all current and prospective employees, and remove access to systems and information for employees who fail verification.
- **Policies/training:** The service provider was contractually required to: (1) implement policies and procedures for employees to protect personal information; (2) implement policies and procedures for physical security management; (3) provide specified training and refresher training to employees; and (4) comply with specified information security practices.
- **Work environment controls:** The service provider was contractually required to use physical and organizational methods to control its work environment to prevent employees from unauthorized access, use, disclosure or retention of personal information.
- **Cybersecurity:** The financial institution and the service provider implemented numerous physical and technological measures to limit access to and protect personal information and the service provider's information technology systems. The service provider was contractually required to comply with specified security requirements and industry standards, and compliance was subject to independent third-party certification.

- **Proactive monitoring/enforcement:** The contract allowed the financial institution to protectively monitor and audit the service provider to ensure contractual compliance, and contained provisions to address non-compliance. The financial institution conducted regular audits and other monitoring activities.

The Report concludes that the financial institution's technological controls, contract with the service provider and associated monitoring and enforcement activities adequately protected the personal information that the financial institution transferred to the service provider, and consequently satisfied the financial institution's accountability obligations.

Report of Findings #2020-003 – Customer Call Centre Outsourcing

The Privacy Commissioner of Canada investigated a consumer electronic retailer's outsourcing of its customer support call centre service to a large multinational company that operated call centres worldwide, including in India. The investigation resulted from customer complaints that the retailer had insufficient security safeguards resulting in the unauthorized disclosure of their personal information to fraudsters who used the information to make targeted "tech support scam" calls to the customers.

The retailer acknowledged that employees at an Indian call center twice circumvented data security measures and misappropriated customer information that they sold to a third party. The retailer argued that it could not prevent rogue employees from misusing their appropriate role-restricted authorized access to personal information to commit criminal data theft. The retailer had security safeguards in place to protect customer information transferred to the service provider, including:

- **Contract:** The service provider was contractually required to implement physical, organizational and technological safeguards to protect customer information. For example, the service provider was required to: (1) restrict logical and physical access to customer information to authorized employees; (2) refrain from printing, saving, copying or storing any customer information except temporarily when needed for business purposes; (3) refrain from removing or transmitting any customer information except with the retailer's permission and, if doing so, to ensure the use of secure encryption technology; (4) implement authentication and access control mechanisms, and personnel security and integrity controls (including background checks); and (5) provide personnel with annual training regarding information security safeguards.
- **Access:** Call centre employees accessed customer information through secure systems that limited access based on their roles and responsibilities. Other access safeguards included limiting the number of users, restricting the availability of certain information and limiting the number of employees who could access and develop reports containing customer information.
- **Cybersecurity:** The service provider used data leakage software that scanned outbound emails for potentially confidential information, and systems to capture queries to support forensic investigations. Physical protections included metal detector screening for all call centre employees and a requirement that they keep personal possessions in lockers outside of active work areas.
- **Proactive monitoring/enforcement:** The retailer had contractual rights to proactively monitor the service provider's security practices. The retailer engaged in periodic audits of the service provider's security practices, and retained an independent expert to conduct a forensic analysis of certain systems.
- **Security incidents:** The service provider was contractually required to promptly report security breaches to the retailer.

The Privacy Commissioner's Report explained that the retailer was required to ensure that its service provider had stringent security safeguards to protect customer information given the sensitive nature of the information, the heightened risk environment and the potential harm to individuals in the event of a breach. The Privacy Commissioner concluded that the retailer's security safeguards were insufficient given the sensitivity of the customer information transferred. In particular:

- **Access:** The service provider's role-based access controls gave too many employees access to customer information, and authorized employees had access to more customer information than was necessary for their job-related functions.
- **Logging/monitoring:** The retailer and service provider did not regularly monitor employee access to customer information. The service provider did not use an active monitoring system to detect anomalous employee access to customer information. The service provider's data leakage software only detected large email attachments, and was easily circumvented by emailing smaller amounts of data.
- **Storage devices:** The retailer did not restrict the use of portable USB storage devices to prevent employees from removing customer information.

- **Breach investigation:** The retailer did not promptly and thoroughly investigate customer complaints about potential personal information security breaches to identify and remediate potential security vulnerabilities.

The Privacy Commissioner's preliminary report recommended the retailer implement enhanced security safeguards to protect customer information and improved procedures for responding to privacy complaints. The retailer agreed to comply with all recommendations.

Comment

Outsourcing arrangements that involve the processing of personal information are increasingly common and important for many Canadian organizations. Outsourcing can provide significant benefits, but it can also present potentially significant business and legal compliance risks.

The Privacy Commissioner's investigation reports demonstrate the Privacy Commissioner's general approach when determining whether an outsourcing arrangement complies with PIPEDA. In summary:

- **Contract:** The Privacy Commissioner will assess the adequacy of the organization's contract with the service provider, including whether the contract adequately addresses legal compliance issues identified by the organization during its pre-contract due diligence investigations.
- **Safeguards:** The Privacy Commissioner will assess the physical, organizational and technological measures (including procedures for responding to potential data security incidents) used to protect personal information transferred to the service provider (including information remotely accessible by the service provider), and determine whether those measures are adequate for the sensitivity of the personal information and consistent with previous Privacy Commissioner guidance and industry best practices.
- **Monitoring:** The Privacy Commissioner will determine whether the organization has adequately monitored the service provider's performance and compliance with contract requirements, and promptly taken steps to remedy identified deficiencies.

PIPEDA does not require perfect safeguards that eliminate all risks to the security of personal information transferred to a service provider. Nevertheless, it may be difficult for an organization that suffers a data security incident to overcome hindsight bias and establish that its outsourcing arrangement complied with PIPEDA's accountability and safeguards requirements. Organizations that outsource the processing and storage of personal information should be mindful of that potential difficulty, and make informed risk-based business decisions about establishing and maintaining their outsourcing arrangements. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's national Cybersecurity, Privacy and Data Protection Group offers comprehensive advice on compliance with privacy laws at the federal and provincial levels as well as with European data protection legislation. We provide both proactive compliance advice and legal advice to help respond to a contravention of privacy laws.