Bulletin | Cybersecurity, Privacy and Data Protection

March 2023

Less is more – Data minimization and privacy/cyber risk management

Data minimization is a fundamental principle of Canadian personal information protection laws and can reduce privacy and cyber risks. Consequently, Canadian organizations should establish and implement written policies and procedures to minimize the personal information they collect and retain.

Data minimization

Data minimization refers to limiting the collection of information to that which is necessary for specified purposes and disposing of information that is no longer required for the purposes for which it was collected. Information should not be collected or retained on a "just in case" basis.

Data minimization is reflected in the *Fair Information Principles*, which are the foundation of Canadian private sector personal information protection laws. For example, the federal *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") includes the following restrictions/requirements:

> *"Principle 4 – Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. … Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. …*
>
> *Principle 5 – Limiting Use, Disclosure, and Retention: … Personal information shall be retained only as long as necessary for the fulfilment of [the purposes for which it was collected]. … Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information. …"*

Similar restrictions/requirements are found in the private sector privacy statutes of Alberta, British Columbia, and Québec, and in the proposed new federal *Consumer Privacy Protection Act (Bill C-27)*.

Data minimization restrictions/requirements are also found in the European Union's *General Data Protection Regulation (GDPR)*, the *California Consumer Privacy Act* as amended by the *California Privacy Rights Act*, and the New York State Department of Financial Services *Cybersecurity Requirements for Financial Services Companies*.

Regulatory guidance and findings

The Office of the Privacy Commissioner of Canada (OPC) has issued guidance for compliance with data minimization restrictions/requirements, including *PIPEDA Fair Information Principle 4 – Limiting Collection*, *PIPEDA Fair Information Principle 5 – Limiting Use, Disclosure, and Retention*, and *Personal Information Retention and Disposal: Principles and Best Practices*. Data minimization restrictions/requirements are also discussed in *Getting Accountability Right with a Privacy Management Program*, issued jointly by the OPC and the Offices of the Information and Privacy Commissioners of Alberta and British Columbia.

The OPC's *Personal Information Retention and Disposal: Principles and Best Practices* explains that "[t]here is no 'one size fits all' retention period" for all information and all organizations, and provides guidance to help organizations determine appropriate retention periods.

The OPC has issued numerous findings of contraventions of PIPEDA's data minimization restrictions/requirements. For example:

- A coffee shop franchisor was found to have contravened PIPEDA because its mobile app collected vast amounts of sensitive location information that was never used for the stated purpose of improved targeted advertising.
- A hotel chain was found to have contravened PIPEDA because it retained guests' personal information longer than necessary for legal compliance purposes and longer than required by its own data retention policy.
- A telecommunications firm was found to have contravened PIPEDA because it retained, without any reason, a database of voiceprints of customers who had opted out of its voiceprint-based biometric authentication program.
- A short-term lender was found to have contravened PIPEDA because it collected more personal information (e.g., loan applicants' banking credentials) than was necessary for the stated purpose of identity verification.
- A rental equipment store was found to have contravened PIPEDA because its practice of collecting copies of customers' driver's licenses was not necessary for the stated purpose of managing risks of lost or stolen equipment.
- A social networking site was found to have contravened PIPEDA because it retained former users' personal information indefinitely and without periodic review and disposal.
- A public opinion research firm was found to have contravened PIPEDA because it collected participants' full birthdate when less information (i.e., month and year of birth only) would have been sufficient for the stated purpose of avoiding fraudulent responses.
- A retailer was found to have contravened PIPEDA because it collected and indefinitely retained customers' driver's license numbers and other government identification numbers for return-of-goods transactions without any persuasive business reason.

Privacy/cyber risk management

Data minimization is an important privacy and cyber risk management practice because the less personal information an organization collects and retains, the less personal information is vulnerable to data security incidents and the less effort and cost will be required to safeguard the personal information or respond to data security incidents.

The amount of data affected by a data security incident will directly affect the cost of responding to the incident, including:

- complying with legal reporting/notification obligations (e.g., investigating the incident, identifying affected personal information and affected individuals/organizations, assessing the risk of harm, and delivering notices to affected individuals and organizations);
- mitigating losses (e.g., restoring affected personal information or paying a ransom for the decryption of personal information or the deletion of exfiltrated personal information);
- mitigating risks of legal claims by affected individuals (e.g., offering free-of-charge credit monitoring/fraud prevention services); and
- defending/settling legal claims by affected individuals and organizations.

The *Ponemon Institute/IBM 2018 Cost of a Data Breach Study: Global Overview* explains:

> *"The more records lost, the higher the cost of the data breach. … In this year's study, the cost ranged from $2.1 million for incidents with less than 10,000 compromised records to $5.7 million for incidents with more than 50,000 compromised records. Each year, the findings show a consistent relationship between cost and size of the data breach."*

The OPC has emphasized that data minimization, including establishing and implementing appropriate information retention/disposal policies, can reduce the scale and impact of a data security incident. For example, *PIPEDA Report of Findings #2007-389* explains:

> *"… maintaining custody of large amounts of sensitive information can be a liability, particularly if the information does not meet any legitimate purpose or if the retention period is longer than necessary. … Collecting and retaining excessive personal information creates an unnecessary security burden. Thus, organizations should collect only the minimum amount of information necessary for the stated purposes and retain it only for as long as necessary, while keeping it secure.*
>
> *… One of the best safeguards a company can have is not to collect and retain unnecessary personal information. This case serves as a reminder to all organizations operating in Canada to carefully consider their purposes for collecting and retaining personal information and to safeguard accordingly."*

See also *Retaining only what is necessary for as long as necessary can reduce impact should a privacy breach occur* and *PIPEDA Findings #2022-005*.

Comments/recommendations

For both privacy law compliance and privacy/cyber risk management reasons, Canadian organizations should:

1. Collect personal information only if and to the extent necessary for identified purposes.
2. Retain personal information only for as long as necessary for the identified purposes for which it was collected or related business and legal compliance purposes.
3. Securely dispose of or anonymize personal information that is no longer required for the identified purposes for which it was collected or related business and legal compliance purposes.
4. Establish, implement and periodically review/update internal written policies and procedures for the collection, retention, and disposal of personal information.

For most organizations, the benefits of data minimization will more than justify the costs. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's national Compliance with Privacy and Data Protection group includes lawyers, located in BLG's offices across Canada, with expertise in Canadian and international privacy laws, cyber risk management and class action litigation. We provide both proactive compliance advice and legal advice to help respond to a privacy breach or resolve privacy disputes. Additional information about BLG's national Compliance with Privacy and Data Protection group and our services is **available here**.

blg.com | Canada's Law Firm
Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.

This document provides general information only, and does not constitute legal or other professional advice. Readers are encouraged to obtain legal advice from a competent professional regarding their particular circumstances.

© 2023 Borden Ladner Gervais LLP. BD11323–03–23

Borden Ladner Gervais