AUGUST 2017

CYBERSECURITY BULLETIN

Borden Ladner Gervais

Less is More – Data Minimization and Cyber Risk Management

Data minimization is a fundamental principle of Canadian personal information protection laws, and can be an effective way to reduce cyber risks. 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 the practice of limiting the collection and retention of information to that which is directly relevant and necessary for a specified purpose. Data minimization is reflected in the *Fair Information Principles*, which are the foundation of Canadian personal information protection laws. For example, the Canadian *Personal Information Protection and Electronic Documents Act* ("PIPEDA") includes the following 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. …*

Data minimization is also a fundamental principle of the European Union *General Data Protection Regulation* ("GDPR"), which goes into effect in May 2018 and includes the following requirements:

> *Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.*
>
> *Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.*

Canadian privacy commissioners have issued findings that criticize Canadian organizations for failing to comply with data minimization requirements. For example, after Winners and HomeSense retail stores in Canada and elsewhere suffered a data breach that affected millions of credit card accounts, the Privacy Commissioners of Canada and Alberta found that the store operators violated data minimization requirements by collecting and retaining certain personal information (e.g. drivers' license numbers) that was not reasonably necessary for relevant transactional purposes. Similarly, after the Ashley Madison discreet affair website suffered a data breach that affected approximately 36 million user accounts, the Privacy Commissioners of Canada and Australia found that the website operator violated data minimization requirements by indefinitely retaining information of users whose accounts were deactivated.

Data minimization does not necessarily require the deletion of personal information when it is no longer necessary for the purpose for which it was collected. Instead, the data can be modified (e.g. aggregated or otherwise anonymized) so that it no longer constitutes personal information. The *Big Data Guidelines* issued by the Information and Privacy Commissioner of Ontario explain that the anonymization of data can be an important mitigation measure to help resolve the tension between data minimization requirements and the desire to use big data.

The Office of the Privacy Commissioner of Canada has issued guidelines titled *Personal Information Retention and Disposal: Principles and Best Practices* to help organizations develop and implement personal information retention and disposal practices that comply with legal requirements for the secure disposal of personal information.

Cyber Risk Management

Data minimization can be an effective cyber risk management practice, because the less personal information an organization collects and retains, the less personal information will be 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 *Ponemon Institute 2017 Cost of Data Breach Study (Canada)* (based on data security incidents suffered by 27 Canadian companies from 12 different industry sectors) found as follows:

> *The more records lost, the higher the cost of the data breach. In this year's study, the average total cost ranged from $3.81 million for data breaches involving 10,000 or fewer compromised records to $7.25 million for the loss or theft of 25,001 to 50,000 records.*

The importance of data minimization as a cyber risk management practice was emphasized by the Privacy Commissioners of Canada and Alberta in their 2007 joint findings regarding the Winners and HomeSense data breach. The Privacy Commissioners stated:

> *TJX/WMI's experience illustrates how 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.*

Final Thoughts

For legal compliance and cyber risk management purposes, Canadian organizations should establish and implement written policies and procedures that comply with data minimization requirements. In particular, organizations should collect personal information only when necessary for legitimate business purposes, and should securely dispose of, or effectively de-identify, collected personal information when it is no longer required for the purposes for which it was collected. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's Cybersecurity Law Group assists clients with legal advice to help manage cyber risks and to respond to data security incidents. Information about BLG's Cybersecurity Law Group is available at blg.com/cybersecurity.

BLG Cybersecurity Group – Key Contacts

Bradley J. Freedman	Vancouver	604.640.4129
Éloïse Gratton	Montréal	514.954.3106
Kevin L. LaRoche	Ottawa	613.787.3516
David Madsen	Calgary	403.232.9612
Ira Nishisato	Toronto	416.367.6349

BLG Vancouver
1200 Waterfront Centre, 200 Burrard St
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415
blg.com