OCTOBER 2017

CYBERSECURITY BULLETIN

Borden Ladner Gervais

The European Union General Data Protection Regulation – A Primer for Canadian Organizations

The European Union *General Data Protection Regulation* (the "GDPR"), which will come into force in May 2018, is a significant evolution in personal data protection laws, and is materially different in important respects from the Canadian *Personal Information Protection and Electronic Documents Act* and similar provincial laws. The GDPR is complicated and nuanced, with permitted variances among European Union ("EU") member states. The GDPR provides regulators with significant investigation and enforcement powers and the ability to impose potentially severe financial penalties for non-compliance.

The GDPR will apply to Canadian organizations that have an establishment in the EU or that collect or process personal data of EU residents in connection with an offering of goods/services or to monitor EU residents' behaviour. Compliance with Canadian personal information protection laws will not satisfy GDPR requirements. Consequently, preparing for compliance with the GDPR may require significant effort, time and expense, and may involve changes to business models and corporate structures. Canadian organizations should determine whether they will be subject to the GDPR, and obtain appropriate technical and legal advice for GDPR compliance.

Some Highlights of the GDPR

Following are some highlights of the GDPR.

1. General

Commencing May 25, 2018, the GDPR will come into force in all EU member states in place of laws that implemented the 1995 *EU Data Protection Directive*. In September 2017, the United Kingdom government proposed a Data Protection Bill, which is similar to the GDPR and will apply after Brexit.

2. Broad Definitions – Personal Data and Processing

The GDPR broadly defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"), and includes data about an organization's own employees. The GDPR broadly defines "processing" as any operation (e.g. collection and storage) performed on personal data.

3. Application to Organizations Inside and Outside the EU

The GDPR will apply to the processing of personal data relating to the "activities of an establishment" (a broad concept) of an organization in the EU, regardless of the location of the data processing. The GDPR will also apply to the processing of personal data by any organization that does not have a presence in the EU if the processing relates to either: (a) an "offering of goods and services" (no payment required) to individuals in the EU; or (b) the monitoring (including for purposes of targeted advertising) of the behaviour of individuals in the EU.

4. Data Controllers and Data Processors

The GDPR will impose obligations and liabilities directly on both data controllers (organizations that determine the purposes and means of processing personal data) and data processors (organizations that process personal data on behalf of data controllers). Data processors must comply with various restrictions/requirements (e.g. process data only as instructed by data controller, use appropriate safeguards, return/delete data when processing is complete, notify data controller of data breaches and no subcontracting without data controller's permission). The GDPR specifies detailed requirements for contracts between data controllers and data processors.

5. Enforcement/Financial Sanctions

The GDPR will be subject to enforcement by "supervisory authorities" with broad investigative, corrective and advisory powers, including the ability to impose on a non-compliant organization administrative fines of up to the higher of €20 million or 4% of worldwide annual turnover/revenue of the organization's undertaking (corporate group) during the previous financial year. In addition, individuals who suffer "material or non-material damage" as a result of a GDPR breach can bring a private lawsuit for compensation, and can be represented in litigation by an authorized public interest organization.

6. Lawful Data Processing/Consent

The GDPR provides that an organization's processing of personal data will be lawful only if and to the extent that the processing is based on one or more specified circumstances (e.g. to perform a contract with the data subject or to take requested steps before entering into a contract, to comply with a legal obligation, to protect the vital interests of the data subject or another natural person, or for the organization's legitimate interests that are not overridden by the data subject's interests or fundamental rights and freedoms) or the data subject has consented to the processing of his or her personal data for a specified purpose.

The GDPR narrowly defines "consent". It must be a freely given, specific, informed and unambiguous indication of consent by a statement or a clear affirmative action. There are additional requirements for children's consent. The GDPR does not contemplate implied consent. In some circumstances, the GDPR requires "explicit" consent. Consent must be easy to withdraw at any time. A request for consent must be unbundled and in clear/plain language. An organization has the burden of proving consent.

7. New Rights/Protections

The GDPR will give data subjects new rights and protections, including:

- **Data Portability:** A data subject's right to receive their personal data and to transmit the personal data to another data controller.
- **Erasure (Right to be Forgotten):** A data subject's right to have a data controller erase their personal data in certain circumstances.
- **Direct Marketing:** A data subject's right to object to the use of their personal data for direct marketing and related profiling.
- **Automated Decision Making (Profiling):** Restrictions/requirements or prohibitions regarding automated decision-making (including profiling) in certain circumstances.

8. Accountability/Governance

The GDPR will require organizations to establish and document a comprehensive data protection program for GDPR compliance, including data protection "by design and by default", data protection impact assessments for high-risk data processing, and detailed records of data processing activities.

9. Other Highlights

The GDPR includes other notable restrictions/requirements, including:

- **Data Breach Notification Obligations:** A data controller must give notice of a personal data breach to the relevant supervisory authority and relevant data subjects without undue delay, and where feasible within 72 hours, after first becoming aware of the breach, unless the breach is unlikely to result in a risk to data subjects' rights and freedoms. A data processor must give notice of a personal data breach to the relevant data controller without undue delay after first becoming aware of the breach.
- **Transparency/Information:** A data controller must provide data subjects with detailed information about the organization's personal data handling practices and related matters.
- **Data Protection Officer:** An organization must designate a data protection officer ("DPO") in certain circumstances. A DPO must have expert knowledge of data protection laws and practices and the ability to fulfil specified tasks (including monitoring compliance with the GDPR), and must be given specified responsibilities and resources.
- **Data Transfers:** There are detailed restrictions/requirements for international transfers of personal data.
- **Special Kinds of Data:** There are prohibitions or stricter requirements for the processing of certain categories of personal data (e.g. genetic data, biometric data and health data).

10. Harmonization with Variations

The GDPR is intended to harmonize data protection laws across the EU, but permits potentially significant variations (procedural and substantive) among EU member states, which may complicate GDPR compliance.

Comment

Many Canadian organizations will be subject to the GDPR, either because they have an establishment in the EU or they collect or process (on their own behalf or on behalf of another organization, including a corporate affiliate) personal data (including employee data) of EU residents in connection with an offering of goods/services or to monitor EU residents' behaviour. The GDPR is materially different in important respects from Canadian personal information laws. Consequently, Canadian organizations should not rely on compliance with Canadian personal information protection laws as sufficient for compliance with the GDPR, particularly in light of the potentially severe financial penalties for noncompliance. Instead, Canadian organizations should now be taking steps, with appropriate technical and legal advice, to prepare for compliance with the GDPR and continued compliance with Canadian personal information protection laws. ■

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

Borden Ladner Gervais

BORDEN LADNER GERVAIS LLP
LAWYERS | PATENT & TRADEMARK AGENTS

Calgary
Centennial Place, East Tower
1900, 520 – 3rd Ave S W, Calgary, AB, Canada T2P 0R3
T 403.232.9500 | F 403.266.1395

Montréal
1000 De La Gauchetière St W, Suite 900
Montréal, QC, Canada H3B 5H4
T 514.879.1212 | F 514.954.1905

Ottawa
World Exchange Plaza, 100 Queen St, Suite 1300
Ottawa, ON, Canada K1P 1J9
T 613.237.5160 | F 613.230.8842 (Legal)
F 613.787.3558 (IP) | ipinfo@blg.com (IP)

Toronto
Bay Adelaide Centre, East Tower
22 Adelaide St W, Suite 3400, Toronto, ON, Canada M5H 4E3
T 416.367.6000 | F 416.367.6749

Vancouver
1200 Waterfront Centre, 200 Burrard St, P.O. Box 48600
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415

blg.com