Legal update

What should Canadian businesses know about GDPR

April 2018
Privacy and access to information

The EU General Data Protection Regulation (GDPR) comes into force on May 25, 2018, and will have implications for many Canadian organizations, particularly those controlling or processing personal information in the European Union or of EU data subjects.

The GDPR represents an overhaul of the European Union’s data protection laws and replaces Data Protection Directive 95/46EC and its member state implementing legislation.

The GDPR places onerous accountability obligations on controllers (organizations that determine the purposes and means of processing data) and processors (organizations that actually process the personal data on behalf of controllers).

Below is an overview of the GDPR’s main features.

Application of the GDPR to Canadian organizations

With an expanded territorial scope, the GDPR will apply to many organizations not currently covered by the European data protection legislation. The GDPR will apply to the processing of personal data by any organizations (including Canadian organizations) that are established in the EU, regardless of where data processing occurs. The GDPR will also apply to the processing of personal data by any organization (including Canadian organizations) that controls or processes data in connection with (1) offering goods or services (even without charge) to, or (2) monitoring the behaviour of individuals in the EU.

The scope of the GDPR is broad and could apply to many Canadian organizations. Processing captures any operation performed on personal data, including collection, use, disclosure and storage. For instance, a Canadian website in English allowing purchases in euros and deliveries to European citizens and a Canadian website tracking the behaviour of European citizens through persistent cookies would probably be covered by the GDPR.

There is a prospect that the GDPR may not apply to Canadian organizations that do not envisage offering goods or services in the EU.

Representative in the EU

Any controller or processor not established in the EU that is caught within the GDPR’s scope will have to designate a representative in the EU to act on its behalf. There is an exception where processing is occasional, does not include large-scale processing of special categories of data (such as personal data revealing racial or ethnic origin, political
opinions, religious or philosophical beliefs, trade union membership or data concerning health) and is unlikely to result in a risk to the rights and freedoms of data subjects.

**Consent**

Under the GDPR personal data can be processed only in certain limited, prescribed circumstances (such as for executing a contract or for legitimate purposes) or with consent. There are particular requirements of a valid consent. The GDPR provides that it must be a freely given, specific, informed and unambiguous indication, given by a statement or by clear affirmative action. Consent must be as easy to withdraw as it is to give. Children under 16 will require parental consent.

**Governance and accountability**

Organizations have positive obligations to implement data protection by design and default and must demonstrate compliance with the GDPR and show data protection is taken seriously and given appropriate levels of attention within the organization.

Organizations will be required to appoint data protection officers if: (1) data processing is carried out by a public authority or body; (2) the organization’s core activities consist of processing operations that require regular and systematic monitoring of data subjects on a large scale; or (3) the core activities consist of processing of special categories of data on a large scale (for example criminal convictions or ethnic origin). Data protection officers must be supported in carrying out their functions, should report to the highest level of management and should have expert knowledge of data protection laws and practices.

The GDPR also formalizes the requirement to carry out privacy impact assessments for types of processing likely to result in high risk to the rights and freedoms of any individual, for example, in the context of profiling, if decisions based on such profiles will produce legal effects.

**Data subjects’ rights**

The GDPR gives data subjects various rights over personal data, including:

- the right to have personal data transmitted to the data subject or another controller in a commonly used machine readable format (data portability);
- the right to require the controller to erase personal data in certain circumstances and where the data has been made public to take reasonable steps to inform other controllers that are processing the data of the request for erasure (right to be forgotten);
- the right to receive more information about the controller’s processing (export solution, storage limits) through a subject access request and to provide the information in a commonly used electronic form;
- prohibitions and restrictions in respect of automated decision-making, including profiling (this may affect AI applications);
- the right to transparency, which requires data controllers to provide detailed information about the organization’s personal data handling practices; and
- the right to object to using personal data for direct marketing.

**Breach notification**

The GDPR will introduce a new mandatory breach reporting regime. If a breach occurs:
• the relevant supervisory authority must be notified “without undue delay” and where feasible, within 72 hours after the data controller becomes aware of the breach. Notification will not be required where the breach is unlikely to result in a risk to the rights and freedoms of data subjects;

• the data subjects must be notified “without undue delay” where the breach is likely to result in a high risk to the rights and freedoms of data subjects.

Controllers will have to maintain a breach register.

**Consequences for non-compliance**

Sanctions under the GDPR could be significant for companies found to have violated legal rights and obligations related to data processing. There are two tiers of sanctions:

• serious infringements will attract a penalty which is the greater of 20,000,000 Euros (i.e., approximately $CDN 30,000,000) or 4% of the annual worldwide turnover of the corporate group; and

• lesser infringements will attract a penalty which is the greater of 10,000,000 Euros or 2% of the annual worldwide turnover of the corporate group.

The GDPR will also allow individuals who suffer material or non-material damage due to a GDPR breach to bring a private lawsuit and be represented by public interest organizations.

**Suggestions for Canadian organizations**

While there is overlap between the GDPR and various Canadian privacy laws (including obligations under PIPEDA, PIPA in Alberta and BC, and Quebec’s Act Respecting the Protection of Personal Information in the Private Sector), Canadian organizations may have to take additional steps to control or process the personal information of EU data subjects in compliance with the GDPR. The BC Office of the Information and Privacy Commissioner has also published some guidance on GDPR and parallels between BC’s PIPA and the GDPR.

Canadian organizations should be reviewing their operations to determine whether they are subject to the GDPR, and understand the applicable legal obligations. Given the new Canadian federal breach reporting requirements and those in the GDPR, it may be appropriate to review those processes in any event. Canadian organizations should consider strategies to manage their GDPR exposure.

Ryan Berger
Caroline Deschênes
Amanda Ferriss

For further information, please contact one of the following lawyers:

> Julie Himo 
  Montréal  
  +1 514.847.6017  
  julie.himo@nortonrosefulbright.com

> Robert L. Percival 
  Toronto  
  +1 416.216.4075  
  robert.percival@nortonrosefulbright.com

> Tony A. Morris 
  Calgary  
  +1 403.267.8187  
  tony.morris@nortonrosefulbright.com

> Ryan Berger 
  Vancouver  
  +1 604.641.4956  
  ryan.berger@nortonrosefulbright.com

Norton Rose Fulbright Canada LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright South Africa Inc and Norton Rose Fulbright US LLP are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients.

References to “Norton Rose Fulbright”, “the law firm”, and “legal practice” are to one or more of the Norton Rose Fulbright members or to one of their respective affiliates (together “Norton Rose Fulbright entities”). No individual who is a member, partner, shareholder, director, employee or consultant of, in or to any Norton Rose Fulbright entity (whether or not such individual is described as a “partner”) accepts or assumes responsibility, or has any liability, to any person in respect of this communication. Any reference to a partner or director is to a member, employee or consultant with equivalent standing and qualifications of the relevant Norton Rose Fulbright entity.

The purpose of this communication is to provide general information of a legal nature. It does not contain a full analysis of the law nor does it constitute an opinion of any Norton Rose Fulbright entity on the points of law discussed. You must take specific legal advice on any particular matter which concerns you. If you require any advice or further information, please speak to your usual contact at Norton Rose Fulbright.

© Norton Rose Fulbright Canada LLP 2018