Privacy Law

The GDPR is coming. Are you ready?

The long arm of comprehensive EU privacy legislation can reach across the Atlantic Ocean and grab hold of Canadian companies that fail to comply with it.

Overview

The *General Data Protection Regulation* ("GDPR") is a law that will come into effect on May 25, 2018. Its purpose is to provide a uniform privacy law across all European Union ("EU") member states and aims to protect the personal information of people in the EU.

You might be wondering why your business should care about a law on another continent. Well, the GDPR applies to Canadian businesses that operate within the EU **or** operate outside the EU but offer goods or services (irrespective of payment) to individuals in the EU or monitor their behaviour. If you are a Canadian business subject to the GDPR and fail to comply, it could literally cost you. Fines for non-compliance can be in the millions of euros.

What Does the GDPR Do?

The GDPR spells out the rules for the "processing" of "personal data". This is EU lexicon for what Canadian laws call the collection, use and disclosure of personal information. In the GDPR, personal data is defined as any information relating to an identified or identifiable individual, known as the "data subject". The GDPR also discusses how businesses are expected to safeguard personal data.

The principles that underpin the GDPR are very similar to those that form the foundation of Canada's private-sector privacy law, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). These principles include, among other things, transparency, accountability, consent, data minimization and adequate security measures.

Canada was declared adequate by the EU in 2001 (meanwhile, our neighbour to the south does not enjoy this distinction), meaning that in eyes of the EU, PIPEDA properly protects personal data transferred from the EU to Canada. However, as you will see the GDPR goes beyond transfers of data.

Generally, Canadian companies that comply with PIPEDA need not be too concerned with the GDPR's requirements as they will have a good head start on being GDPR-compliant although they will likely have to step up their privacy practices to meet their obligations under the GDPR.

What Do You Need to Do?

(a) Identify your role

Assuming that the GDPR applies to your business, it is important to determine whether your business is considered a controller or a processor under the GDPR; each designation has specific duties. A controller determines the purpose and means of processing personal data while a processor is responsible for processing personal data on behalf of a controller. The processor/controller designation will not always be clear and a company can be both. For example, a medium-sized manufacturing company uses the services of a third-party to process its customer payment transactions. The manufacturing company is the controller while the third-party payment company is processor (arguably it is also a controller).

Under the GDPR, both the controller and processor have to work together to ensure personal data of data subject is protected.

Here is a brief description of the obligations of each role:

Processors must:

- maintain records of personal data and processing operations
- implement appropriate security measures
- inform the controller immediately of any breach of personal data

Controllers must:

- implement security measures to protect data and data protection policies
- ensure they have arrangements with processors that comply with the GDPR
- report any breach of personal data to the appropriate authority

(b) Pick a basis

Under the GDPR, your business must have a valid lawful basis in order to process personal data. If it does not, your business will be considered to be unlawfully processing it. There are six available lawful bases to choose from. This can be a challenging exercise, but a necessary one, as you must document your lawful basis. At least one of these must apply whenever you process personal data:

- **Consent:** the data subject has given their consent to the processing
- **Contract:** processing is necessary for the performance of a contract
- **Legal obligation:** processing is necessary for you to comply with the law
- **Vital interests:** processing is necessary to protect someone's life
- **Public task:** processing is necessary to perform a task in the public interest
- **Legitimate interests:** processing is necessary for the legitimate interests of a controller or a third party

(c) Know the rights of data subjects

Data subjects have certain rights with their personal data. These rights are not absolute and vary based on the circumstances:

- **Access:** individuals have the right to access their personal data
- **Rectification:** the right to correct personal data if it is inaccurate or incomplete
- **Erasure/the right to be forgotten**: can request their personal data be deleted
- **Restrict processing:** can block or suppress the processing of their personal data
- **Data portability:** allows individuals to obtain and reuse their personal data for their own purposes across different services
- **Objection:** individuals can object to processing based on legitimate interests or public interest bases, direct marketing and processing for research and statistics

(d) Know your obligations

It is mandatory for certain companies to appoint a data protection officer, which is not dissimilar to a privacy officer (if one is appointed under PIPEDA), and conduct a data protection impact assessment, which is a risk assessment meant to flag weaknesses in procedures for processing personal data. Companies might also have to appoint a representative in the EU.

Let Us Help You

While it is clear that certain GDPR requirements are already seen in Canadian law, there is no mistaking that the GDPR adds another layer of data privacy and security requirements to be aware of. Businesses will have to review exactly how they process personal data and amend their procedures and policies accordingly to ensure compliance. We can help your company get there and be GDPR-ready.

Nishi Malik is a member of the Privacy Law Practice.

Pallett Valo Privacy Law Practice

Privacy and data protection are very important considerations for both private and public sector organizations. At Pallett Valo LLP, our Privacy Law Group advises and supports private sector organizations to comply with their obligations under both federal and provincial laws including the: *Personal Information Protection and Electronic Documents Act* (PIPEDA), *Personal Health Information Protection Act, Freedom of Information and Protection of Privacy Act, Municipal Freedom of Information and Protection of Privacy Act, Canada's Anti-Spam Legislation* (CASL) and the *Digital Privacy Act*. We assist our clients in developing privacy policies and practices to meet strategic business needs and to ensure compliance with privacy legislation.

Contact Members of our Privacy Law Practice:

Andy Balaura
abalaura@pallettvalo.com • (905) 273.3022 ext. 225

Joe Conte
jconte@pallettvalo.com • (905) 273.3022 ext. 217

Nishi Malik
nmalik@pallettvalo.com • (905) 273.3022 ext. 315

PALLETT VALO LLP
Lawyers & Trade-Mark Agents