David Young Law
Compliance Bulletin

January 2018

How will the GDPR affect Canadian businesses?

On May 25, 2018 the European Union's *General Data Protection Regulation* ("GDPR")[1] will come into force, with significant impact on businesses around the globe, including Canada. The GDPR is the successor to the EU's *Data Protection Directive*[2], adopted in 1995, and raises the bar for privacy compliance at the same time as enhancing enforcement mechanisms. However it is the GDPR's expanded extra-territorial application and the significantly higher penalties for noncompliance[3]that have gained the attention of businesses and their advisers in non-EU countries, particularly Canada and the United States.

To put the GDPR in Canadian context, it will be remembered that our national privacy law, PIPEDA[4], owes much of its origin to the 1995 Directive which included, as a key provision, restrictions on data transfer to countries not having adequately equivalent privacy protection rules. PIPEDA, in responding to this requirement, adopted as its ten privacy principles, the precepts of "fair information practices" as embodied in the Directive and as originally set out in the OECD's 1980 Privacy Principles[5]. While the GDPR represents a significant advance in the rigour of privacy protections and the mechanisms for ensuring their effectiveness, for the most part its rules can be characterized as incremental to those under the Directive and therefore not unfamiliar to organizations in Canada required to comply with PIPEDA since as early as January 1, 2001.

New compliance requirements

Data Protection Officer. A review of the salient new compliance requirements under the GDPR reveals that many of them are reflected in Canadian privacy law already. An example is the GDPR's new (relative to the Directive) requirement for organizations that regularly process sensitive personal information on a large scale to appoint a "data protection officer". This requirement is equivalent to the requirement under Canadian privacy law for all organizations that process personal information to identify an individual (or office) responsible for the organization's compliance, most frequently titled "Chief Privacy Officer" (or "Privacy Officer", or "Privacy Office").

Breach reporting. However, a number of the GDPR's rules constitute potentially more rigorous, or new, compliance requirements relative to those under PIPEDA. An example is the requirement for reporting

[1] https://www.eugdpr.org/
[2] http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
[3] Administrative monetary penalties may be up to the greater of 20 million Euros (C$30 million) or 4% of annual worldwide revenues, in each case for a single breach.
[4] *Personal Information Protection and Electronic Documents Act*
[5] http://www.oecdprivacy.org/

David Young Law • Hudson's Bay Centre, Suite 3500, 2 Bloor Street East, Toronto, ON M4W 1A8
T. 416-968-6286 • M. 416-318-5521
Privacy and Regulatory Law Counsel • davidyounglaw.ca

of breaches to the relevant "data protection authority", where feasible, within 72 hours of the occurrence. As we know, PIPEDA has been amended to provide for reporting of breaches, as well as notification of affected individuals – another new GDPR requirement. However these new PIPEDA rules (to come into force sometime in 2018) do not stipulate a specific time period for reporting.

Accountability. A key new GDPR compliance requirement is internal organizational accountability, specifically the establishment of a comprehensive data protection program. Such a program must include documented policies and procedures, maintaining detailed records of all data processing activities, conducting privacy impact assessments for high-risk data processing and generally ensuring that all data protection initiatives are guided by the principle of "privacy by design and by default". While some features of this requirement go beyond what is dictated expressly under PIPEDA, Canadian businesses again should not be unfamiliar with this overall dictate which is consistent with guidance issued by the federal and provincial Privacy Commissioners[6].

Substantive privacy rights. The GDPR also stipulates a number of new or enhanced substantive privacy rights for individuals which organizations will need to address and build into their privacy protection procedures, including the following:

Consent - must be a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of his or her personal data and must be given by a statement or a clear affirmative action.

Right to erasure ("right to be forgotten") - broader than under the Directive and not specifically provided for under Canadian privacy laws.

Right of individuals to restrict processing of their data (e.g. as when accuracy is challenged) - expanded.

Data portability – the right of individuals to transfer their data from one data collector to another).

Obligations imposed directly on data processors

An important new rule under the GDPR is that certain obligations are imposed directly on data processors who perform services for data collectors. These obligations include the requirement to enter into a written agreement with the data collector with stipulated privacy protective provisions, and an overall duty of confidentiality respecting the data they hold. As well, data processors must comply with the data collector's instructions, maintain records describing their data processing activities, ensure appropriate security protections, notify the data collector of breaches without delay, appoint a data protection officer, and cooperate with data protection authorities in connection with investigations. All of these requirements constitute direct compliance obligations of data processors which if not complied with may result in regulatory enforcement actions as well as civil lawsuits.

[6] *Getting Accountability Right with a Privacy Management Program*

Application to Canadian organizations

It is the GDPR's expanded extra-territorial reach that causes us to consider how the full scope of the GDPR could apply to Canadian organizations. Under the 1995 Directive, non-EU organizations were required to comply only if they operated or conducted information processing activities through physical facilities within the EU. By contrast, the GDPR will apply to any organization, wherever located, that uses the personal information of EU residents to market products to, or "monitor the behaviour of", such residents. This application extends to the processing of personal information whether within the EU or outside of it, by both data collectors and data processors. Clearly, therefore, the GDPR's reach is significantly broader. Furthermore, in light of the GDPR's imposing obligations directly on data processors, this extra-territorial reach will have implications for data processors located outside of the EU. In such cases, the data processor will be subject to the GDPR's compliance requirements, as well as the data collector.

What constitutes "marketing to" or "monitoring the behaviour of" EU residents? While mere accessibility to purchase products on a website is not sufficient, functionalities enabling EU residents to use a website, such as offering a service in a local language or providing pricing in a local currency, may cause application of the law. Information collected for purposes of behaviour monitoring must relate to activities of persons within the EU. Monitoring may include, for example, internet tracking or data collection for the purpose of profiling. If such activities are performed by a data processor, even if outside of the EU, both the data collector and the data processor will be subject the GDPR[7].

Conclusions

The potential direct application of the GDPR to Canadian and other non-EU businesses and the exposure to significant financial liability for noncompliance requires organizations outside of the EU to consider very closely its requirements, including its extra-territorial reach. The GDPR represents a significant increase in the rigour of privacy protections currently mandated in the EU under the 1995 Directive. While Canadian businesses may take comfort in the fact that much of the thrust of the new regime will be familiar under our existing privacy laws, the GDPR contains many new or enhanced requirements – both substantive and procedural – relative to those under PIPEDA and its provincial counterparts. It behoves organizations potentially subject to its rules to review them in detail and determine where adjustments in their own procedures may be required.

[7] An interesting question is whether there can be a level of data processing that does not meet the threshold of extra-territorial application. For example, if data is simply maintained by a non-EU data processor who performs no active marketing or monitoring services for a data collector, is that data processor subject to the GDPR?

For more information please contact:

David Young 416-968-6286 david@davidyounglaw.ca

Note: The foregoing does not constitute legal advice. Readers are cautioned that for application to specific situations, legal advice should be obtained.