CYBERSECURITY Q&A

What Canadian Companies Need to Know about the EU's New Data Protection Law

By Michael Scherman

Blakes LAWYERS

It is trite to point out that information crosses national borders today at an unprecedented rate and with very few barriers. A consequence of this unconstrained international flow of information is that domestic data protection laws increasingly have implications abroad. The recent overhaul in the European Union's data protection laws is a prime example of this, which will have implications for Canadian organizations of all sizes and types.

Q: What is the GDPR?

A: The *General Data Protection Regulation* (GDPR) was adopted by the European Parliament in April 2016 and comes into force in May 2018 (replacing *Data Protection Directive 95/46/EC* that is currently in force in the EU). One of the GDPR's objectives is to harmonize protections applicable to the processing of personal data across the EU, but it will also have material implications for Canadian organizations.

Canadian organizations will need to assess to what extent the GDPR applies to their activities and what (if any) changes will be required to stay onside of this new EU law.

Q: Does the GDPR apply to my organization?

A: The first step for any Canadian organization is to determine whether the GDPR applies to its activities. The GDPR's territorial scope is not limited to organizations with a physical presence in the EU, nor is it limited to organizations that are actively or intentionally targeting customers or users in the EU. Even without an establishment in the EU, the GDPR will apply to the extent an organization is processing personal data of subjects who are in the EU where the processing activities are related to: (1) offering goods or services to an individual in the EU (including goods and services offered at no charge); or (2) monitoring the behaviour of individuals that occurs in the EU.

As such, many Canadian organizations will find themselves subject to the GDPR notwithstanding that they are only inadvertently or passively operating in the EU, and any third-party processors of EU personal data will be caught even if they are not established in the EU.

Q: If the GDPR applies to my organization's activities, what are my options?

A: If, as a Canadian organization, you find that your activities fall within the GDPR's scope, there are generally two available courses of action. The first is to restrict your activities such that they fall outside of the GDPR's scope. For example, you might restrict your services to non-EU IP addresses or elect not to process personal data from individuals located in the EU. This could be the best option if your EU activities are neither material nor strategic to your organization. If restricting your activities in such a manner is not desirable (or possible), then the only other available course of action is to comply with the terms of the GDPR.

Q: What obligations will apply under the GDPR?

A: The GDPR imposes a number of obligations that do not exist in Canada (or are more onerous than those that do exist) and, as discussed above, these obligations will apply to many Canadian organizations.

Some of the GDPR's notable (or more unique) aspects are:

- **Obligations on Controllers and Processors:** The GDPR imposes statutory obligations on the person who determines the purposes and means of the processing of personal data (controllers), but it also imposes obligations directly on the persons who process data on behalf of the controller (processors). This differs from Canadian privacy laws, which tend to apply directly only to the controllers and the controller is then responsible for their processors' compliance. For example, under the GDPR, there are express restrictions on subcontracting that apply directly to processors.

- **Consent and Other Grounds for Processing:** Personal data can be processed (e.g., collected, stored, used, disclosed, erased) under the GDPR only where certain requirements are met, for example where the data subject has provided consent. "Consent" is relatively narrowly defined in the GDPR and requires a "freely given, specific, informed and unambiguous indication . . . by a clear affirmative action." As such, opt-out consent will not be a valid means for obtaining consent. If consent is not obtained, there are various alternative grounds for processing.
- **Security and Privacy by Design:** Controllers and processors must implement "appropriate technical and organizational measures to ensure a level of security that is appropriate to the risk," taking into account various other considerations set out in the GDPR. There are also positive obligations to implement data protection "by design and by default."
- **Breach Notification:** Following any "personal data breach," a controller must notify the supervisory authority within specific time-frames. Where the personal data breach is "likely to result in a high risk to the rights and freedoms of natural persons," the data subject must also be notified without undue delay.
- **Automated Processing:** There are a number of provisions in the GDPR regarding automated decision-making and "profiling" (i.e., "automated processing of personal data . . . to evaluate certain aspects relating to natural person"). For example, data subjects have rights of notice, access, consent, and objection in connection with automated decision-making.
- **Right to Erasure ("Right to be Forgotten"):** Data subjects have the right to have personal data concerning them erased without undue delay in a number of circumstances, including where it is no longer necessary for the purpose it was collected (though this right is limited, for example, to the extent the information is necessary for exercising the rights of freedom of expression and information and for the establishment, exercise or defence of legal claims).
- **Portability:** Where personal data is processed using automated means, a data subject has the right to receive their personal data in a structured, commonly used and machine readable format.
- **Mandatory Data Protection Officer:** Controllers and processors must designate a "data protection officer" if: (1) the processing is carried out by a public authority or body; (2) their core activities include regular and systematic monitoring of data subjects on a large scale; or (3) their core activities consist of processing on a large scale of certain categories of data (e.g., data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, data relating to criminal convictions). The data protection officer must have "expert knowledge of data protection law and practices," and the GDPR sets out various rights and responsibilities of such person which require him or her to have a significant level of independence.

Q: What is required to transfer EU personal data outside of the EU?

A: In a similar manner as the current *Data Protection Directive*, EU personal data cannot be transferred outside of the EU except in certain circumstances, such as where consent has been obtained from the data subject or where appropriate safeguards have been put in place (e.g., model contractual clauses).

A transfer can also be made to a non-EU country where the European Commission has decided that the destination country ensures "an adequate level of protection," and Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) has been recognized as providing such an "adequate level of protection." Currently, there are only 11 jurisdictions that have been granted this recognition, so Canada has a relatively unique advantage in this regard. While this may change in the future, for the time being, EU personal data can be transferred to organizations in Canada that are subject to PIPEDA without meeting further requirements (e.g., without obtaining consent for the transfer).

Canadian organizations that are not subject to PIPEDA (e.g., public bodies, universities, organizations subject only to provincial privacy legislation) do not benefit from this adequacy recognition and must ensure they have consent for the transfer or other appropriate safeguards in place before transferring EU personal data to Canada.

Also, PIPEDA's "adequacy" status only facilitates the transfer outside of the EU and does not in any way reduce an organization's obligation to comply with the remainder of the GDPR.

Q: As a Canadian organization, how do I approach compliance?

A: For Canadian organizations, a good first step is to assess current policies and practices and identify gaps relative to the requirements of the GDPR. Once these gaps are known, differing strategies can be assessed and a plan can be crafted to achieve compliance in the most efficient manner possible. For example, for one organization it may be more efficient to isolate the data that is subject to the GDPR and implement a compliance plan only in respect of that data. In other organizations this may not be possible and compliance will need to be implemented across the board.

There are numerous similarities between PIPEDA and the GDPR, so Canadian organizations that comply with PIPEDA will have a head start towards GDPR compliance. With that said, various aspects of the GDPR have no equivalent in PIPEDA (e.g., data portability requirements, data protection officer and mandatory breach notification (which is not yet in force under PIPEDA)), and additional effort will be required in those areas.

The GDPR will impose a wide range of new obligations on many Canadian organizations. Because of the breadth of these new obligations, a compliance plan will require input and consideration from stakeholders across the organization. While May 2018 may seem like a long way out, starting this process early will allow sufficient time for organizations to craft robust and lean processes that achieve GDPR compliance without undue cost or complication.