LANGLOIS

AVOCATS - LAWYERS

GDPR and Canada's Privacy Regime: What Are the Differences?

Since its implementation on May 25, 2019, the European Union's *General Data Protection Regulation* (the "GDPR") has become one of the primary references in matters of privacy protection and digital trust.

While it is true that an adequacy decision rendered by the European Commission recognizes that Canada's *Personal Information and Electronic Documents Act* ("PIPEDA") ensures an "adequate" level of protection of personal data, it was rendered pursuant to EU Data Protection Directive 95/46/EC, which has since been replaced by the GDPR.

There are now significant differences between the two privacy protection regimes. Consequently, Canadian organizations subject to the GDPR can no longer assume they are complying with the GDPR merely because they are complying with the rules and principles laid down in PIPEDA. The inverse is also true for EU organizations doing or seeking to do business in Canada.

This article is intended to provide a practical summary of some of the most important differences between the two regimes.[1]

Scope of application

The GDPR applies not only to the processing of personal data by organizations that have a business establishment in the European Union (the "Union") regardless of where the data are processed, but also to the processing of such data by any organization outside the Union in connection with offering goods or services to people in the Union or tracking their behaviour within the Union.[2] Thus, a Canadian business with no establishment in the Union may be subject to the GDPR if the data processing involved meets the criteria for its extra-territorial application.

PIPEDA applies generally to personal information held by private-sector organizations that carry on activities in Canada (other than in the provinces of Alberta, British Columbia and Quebec, which have legislation essentially similar to PIPEDA). PIPEDA also applies to interprovincial or international transfers of personal information.[3] Thus, an organization established in the Union but carrying on commercial activities and having a "real and substantial connection" with Canada must follow Canadian law.

« …businesses do not have to obtain consent if they can show that the processing is necessary for the purpose of pursuing legitimate interests of the controller or of a third party… »

One of the GDPR's innovations, which currently has no equivalent in Canadian law, is that processors are subject to specific obligations and can become directly liable in the event of a contravention of the GDPR. Thus, beyond instances of direct application, any Canadian organization serving clients who are subject to the GDPR, or who themselves serve organizations subject thereto, should anticipate the addition of GDPR compliance requirements as a contractual condition.

Legal bases of processing

Under the GDPR, consent is only one of several legal bases justifying the processing of personal data. For example, businesses do not have to obtain consent if they can show that the processing is necessary for the purpose of pursuing legitimate interests of the controller or of a third party (unless the fundamental rights and freedoms of the data subject are overriding).

In Canada, consent is the cornerstone of the regime for the protection of personal data (where it is known as "personal information"). Without consent, an organization subject to PIPEDA cannot process personal information except in certain expressly specified cases. However, contrary to the GDPR, which requires that consent be expressly given in order to be valid, consent may be implied under Canadian law, if it can be reasonably deduced from the actions or inaction of a person in light of the circumstances and the notion of reasonable expectations.

Rights of data subjects

The GDPR gives data subjects more control over their personal data. In addition to the right to access and to rectify their data, they are entitled to "data portability" (i.e. the right to receive, in a structured, commonly used, machine-readable and interoperable format, the personal data that they have provided to a controller). The GDPR also recognizes the "right to erasure" — also known as the "right to be forgotten" (i.e. an individual's right to have their personal data erased as soon as possible in certain circumstances).

These rights have no equivalent in PIPEDA. However, last October the Office of the Privacy Commissioner of Canada applied to the Federal Court of Canada to obtain clarity on PIPEDA in order to determine if the right to "de-indexing" (i.e. the removal of links from search results without deleting the content itself) exists in Canada.[4] This case, which involves Google, is being followed closely by stakeholders.

Privacy by design

The GDPR includes the concept of "privacy by design", whereby product manufacturers, service providers and producers of software applications must take into account the protection of personal data throughout the whole engineering process for such products, services and applications, including development and design.

This concept is not mirrored in PIPEDA, which is somewhat ironic since this approach is based on principles developed in Canada in the 1990s by Dr. Ann Cavoukian, former Information and Privacy Commissioner of Ontario.

Reporting security incidents

Under the GDPR, the supervisory authority must be informed without undue delay, and if possible within 72 hours, after the controller learns of a breach that is likely to result in a risk to the rights and freedoms of natural persons. The data subjects must also be informed without undue delay if the breach is likely to result in a "high risk" to their rights and freedoms, unless appropriate measures have been taken to ensure their protection.

Under PIPEDA, the Office of the Privacy Commissioner of Canada and the individuals concerned must be informed "as soon as feasible" if it is reasonable in the circumstances to believe that the breach creates a "real risk of significant harm" to the individuals. The concept of "significant harm" is broadly defined, and includes bodily harm, humiliation, damage to reputation or relationships, financial loss, identity theft, negative effects on the credit record, damage to or loss of property, and loss of employment, business or professional opportunities.

In the event of a breach compromising personal information, organizations must therefore be aware that more than one reporting regime may apply, each with its own particularities (applicable time limits, types of information to be provided, to whom, etc.).

Enforcement powers and sanctions

The GDPR confers extensive enforcement powers on the supervisory authority which, in addition to the imposition of administrative fines, include the following:

- conducting investigations in the form of data protection audits;
- imposing temporary or permanent restrictions, including a prohibition, on processing data;

- ordering the controller to notify the data subjects of a breach of personal data;
- ordering the rectification or deletion of personal data, or restrictions on the processing thereof;
- ordering the suspension of data transfers to a transferee in a third country or to an international organization.

Contraventions of the GDPR can result in costly administrative fines, commensurate with the seriousness of the breach, which can be as high as 20,000,000 euros (about CA$30 million) or, if greater, 4% of an organization's worldwide annual turnover, if the organization commits a particularly serious breach (such as a breach of the conditions for obtaining consent, a breach of the rights of data subjects, or the breach of an order prohibiting data transfers outside the Union or to an international organization).

This past January 21, France's CNIL (*Commission nationale de l'informatique et des libertés*) imposed a €50,000,000 financial penalty against Google for repeated breaches of the GDPR, due to lack of transparency, inadequate information and lack of valid consent regarding the personalization of ads.[5]

« Contraventions of the GDPR can result in costly administrative fines… »

Under PIPEDA, the Office of the Privacy Commissioner of Canada does not have such extensive powers. It does have broad investigatory powers, such as the power to summon witnesses to appear before the Commissioner and to compel them to give evidence. It may also, at any reasonable time, enter any premises occupied by an organization. But once the investigation is over, the Commissioner can only issue recommendations to the organization under investigation. If the latter fails or refuses to implement them, the Commissioner must apply to the Federal Court for an order compelling the organization to follow the recommendations.

Conclusion

In today's world, issues pertaining to personal data protection, and cybersecurity more generally, go well beyond the technological sphere, for they impact the very manner in which organizations operate and make business decisions. It is thus critical for any businessperson to be aware of the various legal regimes that may apply in the global market. In fact, sound compliance practices in privacy and cybersecurity may represent an undeniable competitive advantage for any business.

Consulting a legal advisor will allow you to fully appreciate the scope and substance of the obligations imposed by the various legal regimes applicable to your organization's activities. It can also help you avoid potentially costly errors and allow you to better respond to the expectations of your clients and business partners.

Authors

Caroline Deschênes, CIPP/C
Lawyer, Partner
T +1 438 844 7827
caroline.deschenes@langlois.ca

Pascal Archambault, CIPP/C
Lawyer
T +1 514 282 7817
pascal.archambault@langlois.ca

Notes

[1] There are other differences, and we encourage you to contact us if you have any questions or would like further information.

[2] The citizenship, residence or other legal status of the person concerned has no impact in these situations. In addition, the processing of personal data of Union citizens located outside the Union does not automatically trigger the application of the GDPR. For more details, refer to the Guidelines 3/2018 on the territorial scope of the GDPR published by the European Data Protection Board.

[3] It also applies to personal information concerning employees of Canadian federally regulated organizations (banks, telecommunications enterprises, etc.) regardless of where they are located.

[4] https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/an_181010/

[5] https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc