SHOULD CANADIANS WORRY ABOUT THE EUROPEAN UNION'S *GENERAL DATA PROTECTION REGULATION* (GDPR)?

PIERRE ANTOINE VAILLANCOURT AND MARCEL NAUD*
ROBIC, LLP
LAWYERS, PATENT AND TRADEMARK AGENTS

With the recent personal data management scandals, the new *General Data Protection Regulation* (GDPR), effective as of May 25 of this year, is timely, at least for EU residents. However, Canadian companies should take an interest in the GDPR since its scope will extend beyond the old continent.

1) What is the GDPR?

The GDPR, as its name suggests, "lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data[1]." It imposes numerous obligations on companies (whether they act as the controller or the processors) in terms of personal data, which are more onerous than those currently in force.

In addition, each supervisory authority, responsible for enforcing the GDPR on the national level, has the power to impose fines for deliberate or negligent violation of the regulation, which may be as high as 20 million euros or 4% of the global turnover of the non-compliant company[2]. Hence the importance of ensuring the compliance of your company, if necessary.

2) Are Canadian companies covered by the GDPR?

The new regulation has effects outside the EU. Thus, the GDPR covers any company (established or not established in the EU) that processes personal data of European residents when this processing occurs in the context of activities aimed at:

a. offering goods or services (even free of charge) to European residents; or

b. monitoring of their behaviour through profiling.

* Pierre Antoine Vaillancourt is a lawyer and Marcel Naud is a lawyer and trademark agent for ROBIC, LLP, a firm of lawyers, patent and trademark agents.
[1] Art. 1 GDPR.
[2] Art. 83 GDPR.

If a Canadian company engages in any of these activities, it is subject to the GDPR and faced with a choice: either it limits its activities so that data from EU residents are no longer processed by the company, or it complies with the obligations imposed by the GDPR, otherwise risking heavy fines.

3) What are the obligations under the GDPR?

The GDPR strengthens existing obligations and imposes new ones. Here is an overview of the obligations that may require the most adaptation.

- **Appointment of a representative[3]:** Companies located outside the EU must appoint a representative in Europe who can serve as a link between the European authorities concerned and the foreign company. Some exceptions are provided, but they appear so restrictive that a company will prefer to err on the side of caution and appoint a representative.

- **Detailed use[4]**: According to a fairly widespread current practice, a company lists the uses of the data in rather vague statements such as "to ensure the proper functioning of the services." This approach is no longer sufficient under the GDPR; companies must spell out the purposes of the processing for which the personal data are intended and the legal basis of this processing.

- **Manifest, free and enlightened consent, given for specific purposes[5]**: The GDPR requires the controller to demonstrate that the data subject has given consent, in a form that clearly distinguishes the consent request from any other question when consent is given as part of a written statement which also concerns other issues. Among other things, companies cannot use a simple notice at the bottom of the screen and presume consent or offer an already checked. In addition, it must be as simple to withdraw consent as it is to give it. The data subject must also be able to accept or refuse individually the different data process operations without the execution of a contract being subject to the consent that would not be necessary for this execution.

- **Data protection by design and by default[6]**: The principles of data protection by design and by default should also be taken into consideration not only at the time of the processing itself, but also when determining the means of such processing through appropriate technical and organizational measures such as "pseudonymization." This also involves the minimization of data, so that only adequate and relevant data is collected, limited to what is necessary for the purpose for which it is processed. A certification mechanism can be used to demonstrate compliance with these requirements, which may be of interest in some circumstances.

[3] Art. 27 GDPR.
[4] Art. 13 c) GDPR.
[5] Art. 7 GDPR.
[6] Ar. 25 GDPR.

- **Responsibility of the controller**[7]: The principle of responsibility of the controller obliges companies to implement appropriate technical and organizational measures to ensure that their data processing is carried out in accordance with the GDPR and that they are able to demonstrate this, given the nature, the scope, context and purpose of the processing as well as the risks (the degree of probability and severity of which varies) for the rights and freedoms of natural persons. Companies cannot adopt a passive or nonchalant attitude toward the protection of these data.

- **Data Protection Officer**[8]**:** Some companies must appoint a Data Protection Officer (DPO). The DPO is an individual whose duties include informing and advising data controllers of their obligations and monitoring compliance with the GDPR. Similar to an ombudsman, he must be independent, that is to say that he receives no instructions from anyone in relation to his duties and cannot be relieved of his duties or penalized because of the exercise of his duties.

Practices to adjust

This overview of the obligations of the new European regulation illustrates the EU's desire to significantly increase the protection of personal data. For companies that are not directly targeted by the GDPR, they still have an interest in adjusting their practices in this area, since it would not be surprising to see other jurisdictions, including Canada, follow suit.

[7] Art. 24 GDPR.
[8] Art. 37 et seq. GDPR.