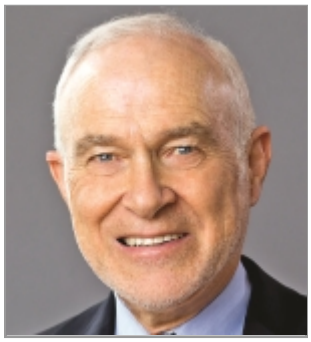
THE LAWYER'S DAILY

The Lawyer's Daily | 111 Gordon Baker Road, Suite 900 | Toronto, ON M2H 3R1 | www.thelawyersdaily.ca
Phone: (800) 668-6481 | Fax: (905) 479-3758 | John.Carson@lexisnexis.ca

Business

GDPR compliance: How Canadian companies should respond

By **David Young**



David Young

(February 20, 2018, 9:03 AM EST) -- On May 25, 2018, some Canadian companies will become directly subject to the European Union's new *General Data Protection Regulation* (GDPR). Others, part of multinational enterprises, likely will align their privacy compliance frameworks with the new EU norms, even if they are not directly subject to the law.

The GDPR is the successor to the EU's 1995 *Data Protection Directive*. While the GDPR will raise the bar for privacy compliance in the EU, its expanded extra-territorial application and significantly higher penalties (up to $30 million or four per cent of annual worldwide revenues) have caught the attention of non-EU companies and their advisers, particularly in Canada and the United States.

Under the 1995 directive, non-EU organizations were required to comply only if they operated or conducted information processing through facilities in the EU. By contrast, the GDPR will apply to *any organization, wherever located*, that uses the personal information of EU residents to market to them or "monitor" their behaviour.

Such extra-territorial reach is not exceptional. To the extent that offshore companies process Canadians' personal information, they are subject to Canada's privacy protection rules even though they have no physical presence here. What is exceptional is the greatly increased risk exposure and the requirements that non-EU businesses adhere to new corporate privacy compliance infrastructure rules in addition to complying with the enhanced privacy protections.

What should Canadian companies be doing to respond to the GDPR? Firstly, they need to assess the likelihood of the GDPR applying to them. Consideration must include whether the company collects, uses or even simply inventories any EU residents' information for marketing or data analysis purposes. The GDPR's further new rule extending application to third party data processors also will need to be considered by service providers to EU entities.

The next step will be to assess where and how their current compliance framework needs adjustment. While the GDPR represents a significant advance in the rigour of privacy protections, for the most part its rules can be characterized as incremental to the 1995 directive. It is therefore not unfamiliar to Canadian businesses, which have been required to comply with our national privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), since as early as Jan. 1, 2001.

In this regard, it is important to note that PIPEDA has been recognized as providing an adequate level of privacy protection relative to the directive. This "adequacy" determination,

one of the original goals of enacting PIPEDA in the late 1990s, permits Canadian organizations to receive and process personal information of EU residents without the need to comply with cross-border privacy procedures such as the "Privacy Shield" which governs data transfers to U.S. companies. PIPEDA's existing adequacy status will continue until it is reviewed under the GDPR, likely to occur sometime over the next two to three years.

While the adequacy status is an important consideration for companies evaluating how they may need to adjust their procedures to respond to the GDPR, it should be understood that this determination directly addresses only the cross-border data transfer issue. If a business will be subject to the new law, based on its extra-territoriality rule, all of the GDPR's requirements must be met, not just the data transfer restriction.

While a review of compliance requirements under the GDPR reveals that many are reflected in Canadian privacy law already, a number are potentially more rigorous. An example is the requirement for reporting of breaches to the relevant regulator within 72 hours. While PIPEDA's new breach reporting rule will come into force sometime later this year, it will not stipulate a specific time period for reporting.

Other examples include the GDPR's enhanced consent rule — requiring a freely given, informed and unambiguous statement or clear affirmative action, and the new right to be forgotten. These rules are not unfamiliar to Canadian privacy law but will dictate a review and potential upgrading of policies and procedures by those companies subject to the GDPR.

In assessing response requirements, a risk assessment may be applied, factoring in the likelihood of regulatory enforcement in the context of the organization's potential exposure to the GDPR and whether its activities are likely to draw the early attention of EU regulators.

The risk assessment should identify procedures that need to be adjusted and "red flagged" to ensure a compliant response if an affected activity is involved. While a full revision of all policies and procedures should be the ultimate goal, an interim "early warning" approach together with a hands-on compliance strategy of learning from received experience and guidance in the early days of the GDPR should enable the company to assess exactly how the new law will require it to respond.

David Young is principal at David Young Law, *a privacy and regulatory counsel practice in Toronto.*

Photo credit / Pe3check ISTOCKPHOTO.COM