Blaney McMurtry LLP

PUBLICATION

New EU General Data Protection Regulation Promises Marked Impact on Canadian Business

Date: June 28, 2018
Author: Dan Giantsopoulos

Original Newsletter(s) this article was published in: Blaneys on Business: June 2018

There has been a recent flood of privacy notifications received from companies updating applicable privacy policies to comply with the European Union's (EU) new General Data Protection Regulation (GDPR), which came into effect at the end of March.

For those who were unaware of these recent EU developments, the GDPR:

- Replaces the EU's previous Data Protection Directive;
- Consolidates and simplifies data protection rules for every company operating in the EU;
- Protects the data privacy of EU residents;
- Provides people living in the EU with more control over their personal data collection;
- Synchronizes data privacy laws across the EU;
- Simplifies the EU regulatory environment for international business, and
- Encourages organizations to reconsider how they handle data privacy.

The GDPR addresses data protection and privacy by regulating and making organizations accountable for how the personal data of people living in the EU is collected and processed. The GDPR mandates that personal data must be protected using the most secure privacy settings, such that it cannot be disclosed publicly without explicit consent from EU residents/consumers.

Personal data is defined as any information that can serve to identify a living individual – either by itself or in conjunction with additional information stored separately. Personal data can only be processed for lawful purposes under the GDPR, or with explicit owner consent, provided that the data owner has the right to revoke consent for data processing at any time. Processing of data includes collecting, using, recording, organizing, storing, retrieving, structuring, altering, adapting, disclosing, destroying, disseminating, restricting, aligning, combining, and more.

The GDPR deals with the:

- Rules for disclosing data security breaches;
- Provision of easy-to-understand terms of service and privacy policies;
- Acquisition of consent from consumers before collecting any personal information, and
- Opportunities available to individuals to obtain, correct, or remove their personal information.

Companies governed by the GDPR must clearly disclose:

- Any data collection or processing;
- The purpose of any data collection or processing;
- How long the data will be retained, and
- If the data will be shared outside the EU or with any third parties.

The GDPR is applicable to any organization that collects personal data from citizens and residents of the EU. As such, Canadian companies who deal with EU customers would be well advised to ensure that they are in compliance with respect to collecting personal data of EU citizens.

This is especially so for Canadian companies that have a physical presence in the EU. The risks for Canadian companies that do not have such a presence might be comparatively smaller but, given the influences of authority, jurisprudence, international law, and international co-operation, the question of how much smaller seems moot.

Under the GDPR, organizations that fail to comply with the GDPR are liable to serious penalties up to a maximum fine of four per cent of annual revenue, or $30.3 million (Canadian dollars) – whichever fee is greater. For most small and medium sized businesses, these fees would prove to be debilitating.

Organizations affected by the GDPR include, but are not limited to:

- Organizations providing online services or sale of products;
- Education providers with students from EU countries;
- Websites using information tracking features, such as cookies, and
- Tourism-related businesses.

The GDPR does not apply in the following situations:

- Deceased persons;
- Legal entities, including national security, military, police, or justice, and
- Statistical and scientific analysis.

Note that the application of the GDPR to Canadian companies is in addition to, and not in replacement of, the data use/collection rules provided by Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) and the privacy legislation provided by the provincial government. PIPEDA was developed to support and promote electronic commerce through governing the processing of personal information in the course of commercial activity.

Similar to the GDPR, PIPEDA ensures individuals can maintain a measure of control over their personal information by prohibiting the inappropriate processing of personal information by

Canadian federal companies, and by mandating rules for safeguarding data as well as disclosing data breaches. PIPEDA also requires that applicable organizations only collect, use or disclose personal information by fair and lawful means for stated and reasonable purposes, and with consent from their customers. Unlike the GDPR, which requires explicit consent, PIPEDA permits consent to be express or implied.

If you are uncertain of how, or if, your business or organization must comply with both the GDPR and PIPEDA, contact Blaney McMurtry LLP for assistance and guidance in navigating the new legislation.

Dan Giantsopoulos is a partner in Blaney McMurtry's corporate/commercial and international trade and business practice groups. His practice focuses on advising a wide variety of businesses corporations (including a wealth of professional corporations), partnerships or joint ventures and their owners/operators in corporate and commercial law, corporate and estate planning and administration, and domestic tax. He is frequently called upon to draft or review Share/Asset Purchase and Sales Agreements, Shareholders' Agreements, Consulting and Employment Agreements; to structure tax-driven corporate reorganizations, and to advise on shareholder disputes. He also advises and represents various American public and private companies with respect to establishing and growing their Canadian business operations.

Dan can be reached at (416) 593-2984 and dgiantsopoulos@blaney.com.

The information contained in this article is intended to provide information and comment, in a general fashion, about recent cases and related practice points of interest. The information and views expressed are not intended to provide legal advice. For specific legal advice, please contact us.