CARTERS
BARRISTERS
SOLICITORS
TRADEMARK AGENTS

# CHARITY & NFP LAW BULLETIN NO. 419

**APRIL 25, 2018**

**EDITOR: TERRANCE S. CARTER**

# IMPLICATIONS OF THE EU'S *GENERAL DATA PROTECTION REGULATION* IN CANADA

***By Esther Shainblum & Sepal Bonni****

## A. INTRODUCTION

The European Union's ("EU") *Regulation 2016/679, General Data Protection Regulation* ("GDPR")[1] will be implemented across the EU as of May 25, 2018. The GDPR harmonizes data protection and privacy laws across all EU jurisdictions and has been referred to by the House of Commons Standing Committee on Access to Information, Privacy and Ethics ("Standing Committee"),[2] as well as the Office of the Privacy Commissioner of Canada ("OPC"),[3] as a point of comparison for Canadian legislation. Of particular note, while the GDPR will apply to organizations with a physical presence in the EU, it has also been given an extraterritorial scope, applying also to organizations that are not established in the EU if they process personal data of EU residents to offer them goods or services (whether or not a fee is charged) or to monitor their behaviour within the EU.[4] Therefore, in certain circumstances, organizations in Canada, including charities and not-for-profits, may be subject to the GDPR and must comply with it, including its breach notification requirements, because of the strict sanctions for non-compliance. Breaches of the GDPR can attract fines as high as €20 million, or up to 4% of the total worldwide annual turnover of the

* Esther Shainblum, B.A., LL.B., LL.M., CRM, practices in the areas of charity and not-for-profit law, privacy law and health law with the Carters Ottawa office. Sepal Bonni, B.Sc., M.Sc., J.D., practices intellectual property, privacy, and information technology law with the Carters' Ottawa office. The authors would like to thank Adriel N. Clayton, B.A. (Hons.), J.D., an associate at Carters Professional Corporation, for assisting in preparing this Bulletin.

[1] *Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, L119, 4/5/2016, p. 1–88 ["GDPR"].

[2] House of Commons Canada Standing Committee on Access to Information, Privacy and Ethics, "Towards Privacy Design: Review of the *Personal Information Protection and Electronic Documents Act*", online: Parliament of Canada <https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/report-12/>.

[3] Office of the Privacy Commissioner of Canada, "Draft OPC Position on Online Reputation" (26 January 2018), online: <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/pos_or_201801/>.

[4] *Supra* note 1, art 3.

preceding financial year, whichever is higher.[5] Additionally, the ramifications of the GDPR's extraterritorial scope also impact "WHOIS" domain name data of EU residents. This Bulletin provides a brief outline of the more prominent changes introduced to privacy law through GDPR, and discusses its application to Canadian charities and not-for-profits, as well as its potential impact on WHOIS domain name search databases.

## B. OVERVIEW OF THE GDPR

The GDPR applies to "processing" of "personal data." "Personal data" is defined as "any information relating to an identified or identifiable natural person" and includes a broad range of identifiers, such as "a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[6] "Processing" of data is also defined broadly and includes any operation performed on personal data, such as "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[7] The GDPR applies to "controllers", *i.e.* natural or legal persons, public authorities, agencies or other bodies that determine the purposes and means of the processing of personal data, as well as "processors", *i.e.* natural or legal persons, public authorities, agencies or other bodies that process personal data on behalf of the controller.[8]

The GDPR strengthens and enhances data protection rights for individuals and imposes strict requirements on organizations engaged in data processing. At a high level, the core principles of the GDPR require that personal data be:

- processed lawfully, fairly and in a transparent manner;
- collected and processed for specified, explicit and legitimate purposes;
- minimized, *i.e.* adequate, relevant and limited to what is necessary in relation to those purposes;
- accurate and kept up to date – inaccurate data must be erased or rectified without delay;

[5] *Ibid*, art 83.
[6] *Ibid*, art 4(1).
[7] *Ibid*, art 4(2).
[8] *Ibid*, art 4(7), (8).

- stored for no longer than is necessary for the purposes; and
- processed in a manner that ensures appropriate security of the personal data.[9]

Organizations to which the GDPR applies must comply with these principles or risk incurring the potentially severe penalties available under it.

Organizations caught by the GDPR must also comply with the enhanced rights for individuals under the GDPR, including the right of access to personal data;[10] providing greater transparency about how data is processed;[11] ensuring data portability rights (*i.e.* the transfer of personal data from one organization to another);[12] the so-called "right to be forgotten" (advising individuals of and complying with their right to request access to and rectification or erasure of personal data, discussed as the "right to erasure" in the March 2018 *Charity & NFP Law Update*);[13] the duty to inform individuals without undue delay of serious data breaches that are likely to result in a high risk to the individual;[14] and ensuring that any consent obtained for the processing of an individuals' personal information is "freely given, specific, informed and unambiguous."[15]

Rules for controllers and processors include the requirement to have a "data protection officer" who is responsible for data protection for businesses that process data on a large scale;[16] a requirement to build data protection safeguards into products and services;[17] requirements for "pseudonymisation" and data encryption where appropriate;[18] breach notification requirements;[19] a requirement to carry out impact assessments when data processing may create a high risk for individuals' rights or freedoms;[20] and the requirement to keep records of processing activities only where processing is regular or likely to create a high risk for individuals' rights or freedoms.

[9] *Ibid*, art 5.
[10] *Ibid*, art 15.
[11] *Ibid*.
[12] *Ibid*, art 20.
[13] *Ibid*, art 13(2)(b). For discussion on the right to erasure, see Esther Shainblum, "House of Commons Standing Committee Report on PIPEDA", *March 2018 Charity & NFP Law Update*, online: <http://www.carters.ca/pub/update/charity/18/mar18.pdf#es1>.
[14] *Ibid*, art 34.
[15] *Ibid*, arts 6(1)(a) and 4(11).
[16] *Ibid*, ch IV s 4.
[17] *Ibid*, art 25.
[18] *Ibid*, arts 25, 32.
[19] *Ibid*, art 33 and 34.
[20] *Ibid*, ch IV s 3.

## C. EXTRATERRITORIAL NATURE OF THE GDPR

As noted above, even if not established in the EU, Canadian charities and not-for-profits may be caught by the GDPR if they process personal data of EU residents to offer them goods or services or to monitor their behaviour within the EU. It is not clear what constitutes "offering goods or services" within the meaning of the GDPR. Merely having a website that is accessible in the EU will not be enough to constitute "offering goods or services."[21] It must also be apparent that the organization "envisages services to data subjects" in one or more EU member states by, for example, mentioning users who are in the EU or using a language or a currency generally used in the EU.[22] "Monitoring behaviour" includes tracking individuals on the internet to analyze or predict their personal preferences, behaviours and attitudes.[23]

Given the vague language of the GDPR, it is possible that, in certain circumstances, organizations in Canada, including charities and not-for-profits, may be subject to the GDPR and must comply with it because of the strict sanctions for non-compliance.

Where the GDPR applies to controllers or processors based outside of the EU, Article 27 of the GDPR requires them to designate a representative within the EU who must be mandated to ensure the controller or processor's compliance with the GDPR.[24] If a Canadian charity or not-for-profit is caught by the GDPR for "offering goods and services" or "monitoring behaviour" in the EU, it will have to designate a representative in the EU, unless it can claim an exemption on the basis that its data processing is "occasional", does not deal with certain categories of particularly sensitive data and does not pose a risk to the rights and freedoms of natural persons.[25]

As noted, administrative fines can be imposed for any infringement of the GDPR. While fines are supposed to be "effective, proportionate and dissuasive"[26], certain infringements are subject to fines of up to €10 million or up to 2% of the total worldwide annual turnover for the undertaking for the previous financial year, whichever is higher.[27] Other more serious infringements, such as non-compliance with the core principles described earlier in this article, are subject to fines of up to €20 million or up to 4% of the

[21] *Ibid*, recital 23.
[22] *Ibid*, recital 23.
[23] *Ibid*, recital 24.
[24] *Ibid*, art 27.
[25] *Ibid*.
[26] *Ibid*, art 83.
[27] *Ibid*.

total worldwide annual turnover for the undertaking for the previous financial year, whichever is higher.[28] Therefore, Canadian charities or not-for-profit organizations who may be caught by the GDPR should implement a plan to bring themselves into compliance as soon as possible.

### D. THE GDPR, DOMAIN NAMES AND TRADEMARK ENFORCEMENT

Regardless of whether or not a Canadian charity or not-for-profit is a controller or processor subject to the GDPR, the GDPR will have implications on "WHOIS" data held by the Internet Corporation for Assigned Names and Numbers ("ICANN") and by the Canadian Internet Registration Authority ("CIRA"). Whereas ICANN's functions include overseeing the coordination and management of the top-level domain name system (*e.g.*, .com, .net, .org, .edu), CIRA is the domain name authority for the .ca top-level domain, managing Canada's internet community policies and representing the .ca registry internationally.

The WHOIS systems maintained by ICANN and CIRA make some personal information (e.g., names, addresses, emails, phone numbers) that is collected when an individual registers a domain name publicly available. WHOIS searches can therefore be used by trademark owners to identify domain name holders in order to enforce trademark rights against them for alleged trademark violations, such as for trademark or domain name infringement.

However, as the WHOIS information held by ICANN and CIRA may include personal information of EU citizens (*i.e.* data subjects) which has been provided in order to register a domain name, ICANN, CIRA and the WHOIS system will be required to comply with the requirements under the GDPR. In this regard, ICANN has stated that while "the extent of the impact of the GDPR on WHOIS and other contractual requirements related to domain name registration data is uncertain", the GDPR will have "an impact at least on open, publicly available WHOIS" data.[29] CIRA has remained relatively silent on the impact of the GDPR on .ca domain names, other than to say that "the rules in Canada are already quite similar to those being put in place in Europe."[30] However, regardless of similarities and differences, CIRA will need to comply with the GDPR with regard to WHOIS data where it is currently not in compliance. Until ICANN and CIRA provide GDPR-compliant solutions, such publicly available data may no longer be

[28] *Ibid*.
[29] Internet Corporation for Assigned Names and Numbers, "Statement from Contractual Compliance", online: <https://www.icann.org/resources/pages/contractual-compliance-statement-2017-11-02-en>.
[30] Canadian Internet Registration Authority, "IT Security Threat Review (From a Canadian Perspective): Data Breaches" online: <https://cira.ca/resources-0/IT-security-threat-review/data-breaches>.

available, which may make trademark enforcement more difficult for Canadian organizations relying on WHOIS data to identify alleged online trademarks violators.

## E. CONCLUSION

The GDPR will introduce sweeping changes to the privacy landscape within the EU with ramifications that will be felt globally as a result of its extraterritorial scope. As these measures will provide individuals with greater rights over the protection of their personal data, organizations will need to ensure that they comply with the GDPR where they are controllers or processors, regardless of jurisdiction. While the Standing Committee has proposed measures in its report, "Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act",[31] that would align PIPEDA with measures in the GDPR on a more domestic level, it remains to be seen whether measures similar to the GDPR will be implemented in Canadian legislation. However, in the meantime, Canadian charities and not-for-profits that may be categorized as controllers or processors should become familiar with the GDPR's regulations and, where necessary, seek legal advice to ensure compliance with the GDPR, particularly given the high potential fines.

In addition to the effects of the GDPR on controllers and processors, any Canadian organizations holding intellectual property should be aware of the GDPR's implications on their ability to enforce trademark rights through the WHOIS system, and should continue to monitor ICANN for updates on its policies. Charities and not-for-profits wishing to enforce trademark rights against domain name holders should act now before this invaluable research tool changes, perhaps forever, and critical domain name registration information is no longer publically accessible.

CARTERS

**Carters Professional Corporation / Société professionnelle Carters** Ottawa · Toronto
Barristers · Solicitors · Trade-mark Agents / Avocats et agents de marques de commerce Mississauga · Orangeville
**www.carters.ca www.charitylaw.ca www.antiterrorismlaw.ca** **Toll Free: 1-877-942-0001**





[31] *Supra* note 2.