CARTERS
BARRISTERS
SOLICITORS
TRADEMARK AGENTS

The 2019 Ottawa Region
Charity & Not-for-Profit Law
Seminar™
February 14, 2019

Critical Privacy Update for Charities and NFPs

By Esther Shainblum, B.A., LL.B., LL.M., CRM

eshainblum@carters.ca
1-866-388-9596

INTRODUCTION

- Significant developments in privacy in 2018
- Big changes both globally and in Canada that:
  - Could change how churches, charities and NFPs in Canada operate
  - Should change how they understand their obligations around privacy, transparency and accountability
- Growing global emphasis on privacy and increasing stakeholder awareness and demands for protection of their personal information
- Expectations that charities must take into account

3

A. SIGNIFICANT DEVELOPMENTS

1. Facebook and Cambridge Analytica

- Facebook allowed 87 million users' personal information ("PI") to be improperly accessed and misused by Cambridge Analytica for political purposes
- Facebook failed to safeguard PI and was not transparent about how it allowed third parties to harvest data on its platform
- Facebook's reputation has been damaged, it was fined and Cambridge Analytica and its parent company have shut down
- Has led to a larger global concern about whether people can trust organizations with their PI

www.charitylaw.ca www.carters.ca

4

www.charitylaw.ca www.carters.ca

5

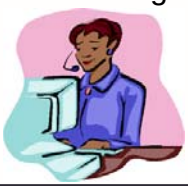
B. THE GENERAL DATA PROTECTION REGULATION ("GDPR")

- The GDPR came into force on May 25, 2018 and harmonizes data protection and privacy laws across all EU jurisdictions
- GDPR strengthens and enhances data protection rights for individuals and imposes strict requirements on organizations engaged in data "processing" - any operation performed on personal data including collection, use, disclosure or storage
- Organizations to which the GDPR applies must comply or face severe penalties

6

1. Why Should Charities in Canada Care About the GDPR?

- Extra-territoriality - GDPR applies 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
  - monitor the behaviour of EU residents within the EU
- Merely having a website accessible in the EU will not constitute "offering goods or services." It must be apparent that the organization "envisages services to data subjects" in the EU



7

- Under the new European Data Protection Board Guidelines (the “EDPB Guidelines”), in order for the application of the GDPR to be triggered
  - There must be an element of "targeting" individuals in the EU, either by offering goods or services to them or by monitoring their behaviour
- The EDPB Guidelines set out factors that indicate that goods or services are being offered, including:
  - Mentioning the EU or a member state by name
  - Giving EU addresses or telephone numbers
  - Using an EU domain name such as “.eu”
  - Mentioning EU customers
  - Using EU languages or currencies
  - Offering delivery of goods in EU member states

www.charitylaw.ca www.carters.ca

8

- If one or any combination of these factors is present with respect to a Canadian charity, the charity may be caught by the GDPR
- The second type of “targeting” activity triggering application of the GDPR is monitoring of data subject behaviour in the EU
- “Monitoring behaviour” includes tracking individuals on the internet to analyze or predict their personal preferences, behaviours and attitudes
- EDPB Guidelines provide that “monitoring” means tracking a person on the internet but can also include tracking through other types of network or technology, such as wearable and other smart devices

www.charitylaw.ca www.carters.ca

9

- EDPB Guidelines - not every online collection or analysis of personal data will automatically count as "monitoring"
  - there must be subsequent behavioural analysis or profiling involving that data, for it to constitute "monitoring"
- But - examples of monitoring activities including "online tracking through the use of cookies or other tracking techniques such as fingerprinting"
- Indicates that using cookies on a website that is accessible to EU residents will be enough to trigger the application of the GDPR, potentially capturing a broad range of Canadian charities
- Other examples of monitoring include targeting advertisements to consumers based on their browsing behavior, CCTV

www.charitylaw.ca www.carters.ca

10

2. Consequences of Breaching the GDPR

- If a Canadian charity is caught by the GDPR due to extra territoriality, it must designate a representative within the EU to oversee its GDPR compliance. Failure to do so is a breach of the GDPR, which could lead to penalties
- A Canadian charity may be exempted from this requirement if it can demonstrate that its data processing is "occasional", does not include large scale processing of certain categories of particularly sensitive data, and is unlikely to pose a risk to the rights and freedoms of natural persons
- Failure to comply with GDPR can lead to fines of 4% of worldwide turnover or €20 million, whichever is higher
- If you think your charity may be subject to the GDPR, obtain legal advice

www.charitylaw.ca www.carters.ca

11

3. Mandatory Breach Reporting

- On November 1, 2018, new breach notification, reporting and recordkeeping obligations came into force under the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") and accompanying regulations
- Must report breaches to the Office of the Privacy Commissioner of Canada ("OPC") and notify affected individual (and possibly third parties) when:
  - an organization experiences a **"breach of security safeguards"** involving PI under its control
  - if it is reasonable in the circumstances to believe that the breach creates a **"real risk of significant harm"** to an individual ("RROSH")

www.charitylaw.ca www.carters.ca

12

- "Breach of security safeguards" means loss of, unauthorized access to or unauthorized disclosure of PI
- "Significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property
- Relevant factors in determining whether a breach of security safeguards creates a RROSH include:
  - the sensitivity of the PI
  - the probability of misuse of the PI
  - any other prescribed factor (none so far)

ES3

www.charitylaw.ca www.carters.ca

Slide 12

ES3 resulting from a breach of or a failure to have physical, organizational and technical security safeguards appropriate to the sensitivity of the information

Esther Shainblum, 10/29/2018

13

- Obligations:
  - report the breach to the OPC;
  - notify the affected individual
  - notify any third party (*e.g.* the police, bank, credit reporting agency) that may be able to reduce or mitigate the harm
- Must retain records of all breaches for 24 months regardless of materiality
- Charities and NFPs should not assume they are exempt from PIPEDA - what constitutes a commercial activity will vary with the facts of each case
- Charities and NFPs should consider voluntary compliance given increasing stakeholder awareness and expectations around privacy, transparency and accountability

14

15

4. New OPC Guidelines

- In 2018 OPC published two new guidance documents to improve compliance with privacy obligations:
  - "Guidelines for obtaining meaningful consent" – effective January 1, 2019
  - "Guidance on inappropriate data practices – effective July 1, 2018

16

- Consent Guidance sets out seven principles to guide organizations in their consent processes, including:
  - provide information about privacy in a clear, comprehensive, understandable and accessible manner
  - allow individuals to control the amount and the timing of detail they receive – *e.g.* layered format
  - use innovative and interactive forms and tools to obtain consent

- Data Guidance identifies a series of principles to protect individuals from inappropriate data practices
- Only collect, use or disclose PI for purposes that a reasonable person would consider appropriate in the circumstances

17

- No-Go Zones, including collection, use or disclosure that is unlawful, unethical or likely to cause harm
- Churches, charities and NFPs should not assume they are exempt from PIPEDA
- These are best practices regarding consent and appropriate data practices in Canada - churches, charities and NFPs should adhere on a voluntary basis

www.charitylaw.ca www.carters.ca

18

C. WHY CHARITIES SHOULD COMPLY WITH PIPEDA

1. Commercial Activity versus Tax Status

- Charities are not automatically exempt from PIPEDA
- PIPEDA applies to any organization that collects, uses, or discloses personal information in the course of commercial activities (s. 2(1))
- What is relevant is the nature of the specific activities undertaken by an organization, not its tax status (as for profit or charity)
- OPC - "whether or not an organization operates on a non-profit basis is not conclusive in determining the application of the Act"

www.charitylaw.ca www.carters.ca

19

- Whether an organization is collecting, using or disclosing personal information in the course of a commercial activity is fact-based
- OPC found that a non-profit daycare organization was caught by PIPEDA
  - payment for child care services was seen as a commercial activity
- OPC found that the non-profit Law School Admission Council was engaged in commercial activity
  - OPC stated that there is no exemption for non-profit or member-oriented organizations

20

- Charities increasingly turning to sale of goods and services methods to earn revenue
  - increasing likelihood that revenue-generating activities may be caught by PIPEDA
- It is becoming increasingly complex for a charity (or the OPC or a court) to determine whether an activity falls within the scope of PIPEDA
- No bright-line test that can be applied to determine whether an activity is commercial in nature. Whether an activity constitutes a commercial activity will vary with the facts of each case

21

- Most prudent for charities to assume that the OPC or a court might find that they are engaged in commercial activity and that they are subject to PIPEDA
- Therefore, charities should obtain consent and abide by the other "fair information principles"
- By complying voluntarily with PIPEDA, charities can also avoid accidentally breaching PIPEDA requirements if their activities turn out to be commercial - avoiding possible fines and penalties

www.charitylaw.ca www.carters.ca

22

2. Public Policy

- No convincing public policy justification for excluding charities from privacy law requirements
- *GDPR* applies to charities and not-for-profits, as does BC *Personal Information Protection Act*, and many charities and not-for-profits are also subject to Alberta *Personal Information Protection Act*
- Many health information custodians under the Ontario *Personal Health Information Protection Act, 2014* and its counterparts in other provinces are charities

www.charitylaw.ca www.carters.ca

23

- Charities and not-for-profits can and do comply with privacy legislation throughout Canada and elsewhere
- Charities across Canada are in control of a great deal of personal information, e.g. donors, clients and volunteers
- Majority of Canadians make financial donations to charities or not for profits
- Majority of Canadians prefer to donate online
- The privacy interests of many Canadians will turn on the nature of the privacy protections, safeguards and protocols that Canadian charities have in place

www.charitylaw.ca www.carters.ca

24

www.charitylaw.ca www.carters.ca

25

3. Stakeholder Expectations

- There are increasing stakeholder awareness and expectations around privacy, transparency and accountability
- Consumers do not expect different standards of protection to apply depending on whether they are providing their credit card number to a charity or to an online retailer
- Stakeholders expect charities to safeguard their personal information, protect it from misuse and be transparent and accountable for how it is used

26

- In the 2018 Global Trends in Giving Report, 92 per cent of donors said it was important for charities to protect their financial and contact information from data breaches
- Charities and not-for-profits should take these expectations into account when developing and adopting their privacy practices
- By aligning with PIPEDA, charities can maintain the trust and confidence of their donors, clients and other stakeholders, and minimize the risk of reputational damage

27

4. Litigation

- Canadian courts showing an increasing willingness to protect privacy interests
- Violations of privacy can give rise to damage awards, tort claims and class action litigation in the courts
- Privacy-related class action litigation on the rise in Canada - *e.g.* multi million dollar Winnipeg Royal Ballet class action brought by former students for intimate photos taken by instructor and posted online

28

- Risks associated with privacy breaches and violations including the risk of court action, class action litigation, court awarded damages and reputational injury
- Floodgates have been opened for new privacy-based lawsuits
- The rise of class action lawsuits to remedy privacy breaches poses an existential risk to all organizations
- The standards set out in PIPEDA will shape stakeholder expectations, and possibly court expectations, regarding how an organization should collect, use, disclose and safeguard personal information

29

CONCLUSION

- There is a growing global emphasis on and regulation of privacy as well as increasing stakeholder awareness and expectations
- Charities and NFPs in Canada should move toward alignment with PIPEDA, including mandatory breach notification and the new guidances, to:
  - Ensure that they are compliant where applicable
  - Meet stakeholder expectations around privacy, transparency and accountability
- The stakes are high - possible reputational damage, loss of stakeholder confidence and possible fines and penalties

www.charitylaw.ca www.carters.ca

CARTERS
BARRISTERS
SOLICITORS
TRADEMARK AGENTS

Disclaimer

This handout is provided as an information service by Carters Professional Corporation. It is current only as of the date of the handout and does not reflect subsequent changes in the law. This handout is distributed with the understanding that it does not constitute legal advice or establish a solicitor/client relationship by way of any information contained herein. The contents are intended for general information purposes only and under no circumstances can be relied upon for legal decision-making. Readers are advised to consult with a qualified lawyer and obtain a written opinion concerning the specifics of their particular situation.

CARTERS PROFESSIONAL CORPORATION
TOLL FREE: 1-877-942-0001
Ottawa Toronto Orangeville
www.carters.ca www.charitylaw.ca www.antiterrorismlaw.ca