CARTERS
BARRISTERS
SOLICITORS
TRADEMARK AGENTS

SPRING 2021 CHARITY & NFP WEBINAR SERIES

***VIRTUAL* – MAY 25, 2021**

OUTSOURCING AND TRANSFERS OF PERSONAL INFORMATION FOR CHARITIES AND NFPS

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

eshainblum@carters.ca
1-877-942-0001

CARTERS
BARRISTERS
SOLICITORS
TRADEMARK AGENTS

CARTERS SPRING 2021
CHARITY & NFP WEBINAR SERIES
Tuesday, May 25, 2021

Outsourcing and Transfers of Personal Information for Charities and NFPs

By Esther Shainblum, B.A., LL.B., LL.M. CRM
eshainblum@carters.ca
1-877-942-0001

Esther Shainblum, B.A., LL.B., LL.M., CRM – Esther practices at Carters Professional Corporation in the areas of charity and not for profit law, privacy law and health law. From 2005 to 2017, Esther was General Counsel and Chief Privacy Officer for Victorian Order of Nurses for Canada, a national, not-for-profit, charitable home and community care organization. Before joining VON Canada, Esther was the Senior Policy Advisor to the Ontario Minister of Health. Earlier in her career, Esther practiced health law and corporate/commercial law at McMillan Binch and spent a number of years working in policy development at Queen's Park.

3

OVERVIEW

- Introduction
- What is Outsourcing and Why Outsource?
- Charities and NFPs in Canadian Privacy Law
- Outsourcing under PIPEDA
- Principles set out in OPC Guidances and Findings
- Mandatory Breach Reporting
- Cloud Computing
- Outsourcing Agreements
- Key Takeaways
- Appendix – Summary of Fair Information Principles

4

A. INTRODUCTION

- Charities and Not-for Profits ("NFPs") frequently contract with third parties to provide them with various services
- Such outsourcing could involve the transfer of personal information ("PI") to the third party provider
- Charities and NFPs need to understand the privacy law implications of outsourcing as well as their legal obligations in relation to any PI that may be transferred in the course of outsourcing
- This presentation will explain the law and provide some practical suggestions

5

B. WHAT IS OUTSOURCING AND WHY OUTSOURCE?

1. What is Outsourcing?

- Charities and NFPs may contract with third parties to provide them with specific services that they either cannot or choose not to perform themselves – *e.g.* online data storage or donor management systems
- Charities and NFPs may also choose to transfer activities or functions to a third party – *e.g.* IT outsourcing, as well as business process outsourcing, such as payroll, back office
- For the purposes of this presentation, "outsourcing" means any such arrangement that involves the transfer of PI

www.charitylaw.ca www.carters.ca

6

2. Why Outsource?

- A charity or NFP may choose to outsource for a number of reasons including:
  - To reduce operating costs
  - To increase efficiency
  - To obtain access to specialized services, expertise or technology
  - To focus on organizational/charitable mission and core competencies
  - To address gaps in the organization

www.charitylaw.ca www.carters.ca

7

C. CHARITIES AND NFPS IN CANADIAN PRIVACY LAW

- Canada's *Personal Information Protection and Electronic Documents Act* ("PIPEDA") applies to any private sector organization that collects, uses, or discloses personal information in the course of "commercial activities"
- There is no test to determine whether an activity is commercial
- Whether something constitutes a commercial activity will vary with the facts of each case

www.charitylaw.ca www.carters.ca

8

- Charities and NFPs are not automatically exempt from PIPEDA, but PIPEDA does not generally apply to charities and NFPs because most of the activities that they regularly engage in do not qualify as "commercial activities"
- To the extent, though, that charities and NFPs are engaging in commercial activities, they must comply with PIPEDA in the course of those activities
- Does that mean that charities and NFPs not carrying out commercial activities have no privacy obligations?

www.charitylaw.ca www.carters.ca

9

- Even if charities and NFPs are not technically subject to PIPEDA, they may still face an environment in which there is:
  - Increasing stakeholder awareness and expectations around privacy, transparency and accountability
  - Recognition of new privacy law torts, increasing the risk of privacy based lawsuits, and increasing willingness of courts to protect privacy interests
  - Increasing incidence of privacy and cyber security incidents, especially since the onset of the pandemic and the consequent surge in cybercrime
  - Increasing risks associated with privacy breaches and cyber incidents, including tort claims, class action litigation, court awarded damages and reputational injury

10

- Under the *Canada Not-for-Profit Corporations Act* ("CNCA"), the *Ontario Not-for-Profit Corporations Act* ("ONCA") (expected to be proclaimed in 2022), and the Ontario *Corporations Act* ("OCA") directors and officers are required to:
  - Act honestly and in good faith with a view to the best interests of the company; and
  - Exercise the care, diligence, and skill that a reasonably prudent person would exercise in comparable circumstances

11

- Directors and officers of charities and NFPs impacted by privacy breaches may be exposed to the risk of litigation and claims that they are liable for the breach
- Directors can show that they met the required duty of care by, among other things, confirming that the organization has appropriate safeguards in place to protect PI and respond to breaches
- ***Takeaway*** - charities and NFPs cannot disregard privacy obligations

12

- Charities and NFPs should consider building and implementing their privacy policies and procedures based on the 10 fair information principles set out in Schedule 1 to PIPEDA, that also underlie other Canadian privacy legislation (see end of this presentation)

- These principles shape stakeholder and could shape regulator/court expectations, regarding how an organization should handle the collection, use, disclosure, and safeguarding of PI

13

- Compliance with the fair information principles positions charities and NFPs to demonstrate good faith, due diligence and maintain donor/stakeholder trust and confidence
- Office of the Privacy Commissioner of Canada ("OPC") recommends that charities and NFPs follow the fair information principles as best practices
- Note that charities and NFPs operating in BC and Quebec and, to some extent in Alberta, are subject to substantially similar provincial privacy legislation that replaces PIPEDA in respect of PI within those provinces

14

- Alberta *Personal Information Protection Act* (PIPA) requires organizations that outsource outside of Canada to provide notice before the transfer as well as certain prescribed information to affected individuals
- Currently in Quebec, PI can only be communicated to third parties outside of the province in certain circumstances. Under Bill 64, its proposed new privacy legislation, Quebec would have stringent requirements for transferring PI outside the province
- An in-depth review of these provincial requirements is beyond the scope of this presentation

15

D. OUTSOURCING UNDER PIPEDA

- "Processing" – any use of the information by the third party processor for a purpose for which the transferring organization can use it. See link for OPC Guidelines https://www.priv.gc.ca/en/privacy-topics

1. Fair Information Principle 4.1.3 Accountability

- "An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing"
- "Outsourcing organizations must use contractual or other means to provide a comparable level of protection while the information is being processed by a third party"

16

2. Fair Information Principle 4.7- Safeguarding

- "PI shall be protected by security safeguards appropriate to the sensitivity of the information"

3. 4.7.3 – The methods of protection should include:

"(a) physical measures *e.g.,* locked filing cabinets and restricted access to offices;

(b) organizational measures, *e.g.,* security clearances and limiting access on a "need-to-know" basis; and

(c) technological measures, *e.g.,* the use of passwords and encryption"

17

E. PRINCIPLES SET OUT IN OPC GUIDANCES AND FINDINGS

- Charities and NFPs subject to PIPEDA or voluntarily complying with fair information principles should refer to OPC for guidance
- OPC - Nothing in PIPEDA prohibits outsourcing the processing of data
- But, organizations must take privacy considerations into account when outsourcing to another organization
- Must take all reasonable steps to protect information from unauthorized uses and disclosures while in the hands of the third party processor
- See link https://www.priv.gc.ca/en/privacy-topics/employers-and-employees/outsourcing/02_05_d_57_os_01/

18

- The outsourcing organization must be satisfied that the third party has policies and processes in place, including training for its staff and effective security measures, to ensure that the information is properly safeguarded at all times

- If outsourcing outside of Canada, the outsourcing organization must use clear and understandable language at the time of collection to advise individuals that their information may be processed in a foreign jurisdiction and may be accessed by authorities in that jurisdiction

19

1. **OPC Guidelines on Processing PI Across Borders**
OPC position since 2009 that transfers of PI for processing are a "use" by the transferring organization and not a "disclosure" and that consent is not required as long as the PI is being used for the purpose for which it was originally collected. For more information on OPC Guidelines see link https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127/

2. **PIPEDA Report of Findings Re: Equifax #2019-001**

- OPC briefly deviated from this position in 2019, finding that transfers of PI for processing were "disclosures" of PI that required express consent

20

- Later that year OPC reverted to position that transfers for processing are "uses" not "disclosures". For more information see link https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/
- Therefore consent is not required to the transfer of PI by an organization to a service provider as long as the PI is being used for the purpose for which it was originally collected
- OPC - Outsourcing organizations should be transparent in handling PI and must advise stakeholders that PI may be sent to another jurisdiction and may be accessed by authorities in that jurisdiction

21

3. PIPEDA Report of Findings Re: TD Canada Trust (TD) #2020-001

- Service provider in India accessing limited PI on a portal constituted a transfer for processing
- OPC found that the consent TD obtained at the time of collection allowed PI to be used for the purpose for which it had been transferred – no additional consent required and no opt-out required
- OPC found TD had been sufficiently open about the transfers of PI for processing with prominent, readily available, clear and understandable information about transfers to service providers in other jurisdictions
- OPC noted robust contracts are especially important when the third-party processor is located in a foreign jurisdiction and not subject to PIPEDA

22

- TD's contract controlled use, access and disclosure of PI by processor and TD also used additional safeguard measures:
  - Risk assessments
  - Employee screening and training
  - Work environment controls – "clean room"
  - Access and other cybersecurity controls to limit access and prevent unauthorized access
  - Proactive monitoring and enforcement of contractual obligations
- OPC found that TD had used contractual and other means to provide a comparable level of protection to that required under PIPEDA for customers' PI being processed by the third-party service provider

23

4. PIPEDA Report of Findings Re: Dell # 2020-003

- Dell outsourced tech support to a call centre in India
- Employees used customer PI to scam Dell customers
- OPC found the PI was sensitive, the call centre was a high risk environment and significant harms could and did arise from a breach
- OPC found Dell's security safeguards were lacking:
  - Access Controls – too many people/too much PI
  - Lack of Monitoring and Logging
  - Technical Measures – no control over use of portable storage devices (USB drives)
  - Inadequate Breach Investigation

24

- Dell agreed to implement OPC recommendations:
  - Thoroughly investigate all complaints and all privacy breaches
  - Training for staff
  - Logging and monitoring to detect anomalous requests for customer PI

- Dell also:
  - Implemented access controls to reduce access to PI
  - Disabled USB functionality and restricted printer access and internet and email access

25

F. MANDATORY BREACH REPORTING

- PIPEDA require organizations that experience certain types of data breaches to report them to the OPC, to notify the affected individuals and, in some cases, to notify third parties such as the police or a credit reporting agency
- The notification requirement is triggered when a "breach of security safeguards" creates a "real risk of significant harm" ("RROSH") to an individual
- OPC Guidance – The organization in control of PI is responsible for mandatory breach reporting

26

- An organization remains responsible for PI it has transferred to a third party for processing and therefore responsibility for reporting rests with the outsourcing organization. For more information, see link https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/
- ***Takeaway*** – If there is a breach creating a RROSH when PI is in the hands of the processor, the outsourcing organization has the legal obligation to report to the OPC, notify the affected individuals and comply with the record keeping obligations under PIPEDA

27

- The outsourcing organization must have contract in place with the processor to require compliance with breach reporting requirements
- Charities and NFPs that are voluntarily complying with the fair information principles should be aware of these requirements and, to the extent that they are carrying out commercial activities, may be required to comply with them
- Case study – Blackbaud Breach
- Note – charities and NFPs subject to Alberta PIPA must comply with its mandatory breach reporting requirements and Quebec will also have mandatory breach reporting requirements if Bill 64 passes

28

1. Blackbaud Breach 2020

- In July 2020, Blackbaud, a cloud based donor management provider, revealed that, two months earlier, it had been the subject of a ransomware attack that impacted many Canadian charities
- Blackbaud initially took the position that it was not required to notify the OPC because it was the processor and therefore not the organization in control of the PI
- All the outsourcing organizations were charities and therefore technically not subject to the breach reporting requirements
- In the interests of transparency with their stakeholders, a number of Canadian charities voluntarily advised their stakeholders even though notification was not strictly required
- Blackbaud eventually sent a courtesy notice to the OPC

29

G. CLOUD COMPUTING

- Many charities and NFPs use cloud based services such as data storage, donor management systems and web hosting services
- In cloud computing, the services delivered to the outsourcing organization may be flowed through servers in different locations/countries
- Most cloud computing contracts are “click-wrap”/take it or leave it and are generally not negotiated

30

- The OPC warns organizations to carefully review the terms of service of the cloud provider and ensure that the PI will be protected in the hands of that provider
- Outsourcing organizations have an obligation to use contractual or other means to ensure that the PI transferred to the cloud provider is appropriately protected
- For more information see link below https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/online-privacy/cloud-computing/

31

H. OUTSOURCING AGREEMENTS

- As we have seen:
  - The outsourcing organization remains responsible for the PI in the hands of the processor
  - The outsourcing organization must use contractual or other means to provide a comparable level of protection while the PI is being processed by the third party
  - PI must be protected by security safeguards appropriate to the sensitivity of the information

32

- Before entering into any outsourcing arrangement, charities and NFPs should:
  - complete a detailed risk assessment to identify any potential privacy risks
  - obtain legal advice on the applicable privacy and information security obligations and considerations
  - incorporate these findings in the outsourcing contract
- Charities and NFPs that wish to outsource must ensure that the outsourcing agreement includes sufficient privacy protections and procedures to allow them to meet their obligations under PIPEDA
- Processors generally have a standard form of agreement that they like to use and prefer not to negotiate them

33

- Outsourcing charities and NFPs should resist signing standardized or "click-wrap" agreements and insist on additional privacy obligations in the agreement, including covenants that the processor will:
  - Handle PI in accordance with applicable Privacy Laws, which should be broadly defined
  - Provide the processing services in accordance with applicable Privacy Laws
  - Collect, use, disclose, store and dispose of PI solely for the purposes of providing the named specific processing services
  - Not disclose PI in contravention of any Privacy Laws
  - Limit access to PI to those of its employees who require it to provide the processing services

www.charitylaw.ca www.carters.ca

34

  - protect PI by implementing security safeguards appropriate to the sensitivity of the PI including, without limitation:
    - Access controls
    - Work environment controls
    - Employee screening and training
    - Thorough and appropriate investigations
  - promptly notify the outsourcing organization of any data/privacy breach including details of the breach
  - not disclose or transfer PI to any subcontractor without consent of the outsourcing organization
- The outsourcing agreement should permit the outsourcing organization to carry out proactive monitoring and enforcement of contractual provisions and other safeguards

www.charitylaw.ca www.carters.ca

35

I. KEY TAKEAWAYS

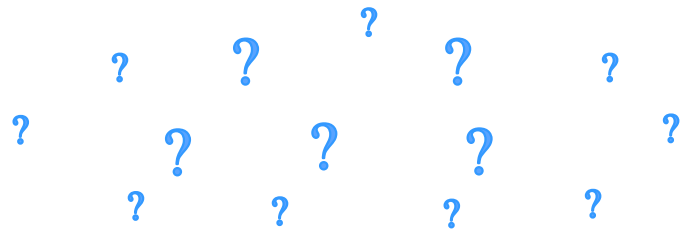
1. Outsourcing charities and NFPs remain responsible for the PI in the hands of the processor
2. Take steps to ensure that the PI will be protected in the hands of the processor
3. Provide readily available, prominent, clear and understandable information regarding transfers of PI for processing
4. Ensure the consent obtained at the time of collection allows PI to be used for the purpose for which it will be transferred

36

5. Carry out risk assessments and obtain legal advice before entering into outsourcing agreements
6. Do not agree to “take it or leave it” standardized contracts and insist on additional privacy obligations in the agreement
7. Implement and enforce contractual safeguards and other safeguard measures
8. Include provisions permitting monitoring and auditing of provider compliance
9. Charities and NFPs in BC, Alberta and Quebec must investigate and comply with their obligations under provincial privacy legislation

37

QUESTIONS?



38

APPENDIX - BRIEF SUMMARY OF THE FAIR INFORMATION PRINCIPLES

1. **Accountability**
   - The organization is responsible for PI under its control and will designate an individual to be accountable for its compliance with these principles
2. **Identifying Purposes**
   - The organization will identify the purposes for which PI is collected at or before the time the information is collected
3. **Consent**
   - The knowledge and consent of the individual are required for the collection, use, or disclosure of PI, except where inappropriate
4. **Limiting Collection**
   - The collection of PI will be limited to that which is necessary for the purposes identified by the organization. Information will be collected by fair and lawful means

39

5. Limiting Use, Disclosure and Retention

- PI will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. PI will be retained only as long as necessary for the fulfillment of those purposes

6. Accuracy

- The organization will take reasonable steps to keep PI as accurate, complete and up-to-date as is necessary for the purpose for which it is used

7. Safeguards

- The organization will take reasonable steps to keep PI protected by security safeguards appropriate to the sensitivity of the information

40

8. Openness

- The organization will make easily available to individuals specific information about its policies and practices relating to the management of PI

9. Individual Access

- Upon request, an individual will be informed of the existence, use, and disclosure of their PI, and will be given access to it. An individual will be able to challenge the accuracy and completeness of the PI and have it corrected as appropriate

10. Challenging Compliance

- An individual will be able to address a challenge about an organization's compliance with the principles to the designated individual(s) accountable for its privacy compliance

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
Toronto Ottawa Orangeville
www.carters.ca www.charitylaw.ca www.antiterrorismlaw.ca