LogicalOutcomes Canada

PIPEDA Report: DRAFT

Audited by: AVAINTCON Consulting

Version 2.0

July 2014

Document Information

Purpose of this Document

The purpose of PIPEDA is to balance individuals' privacy rights with the need of organizations to collect, use or disclose personal information for reasonable and appropriate purposes.

The PIPEDA Act aims to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act.

This Report is focused on the handing of personal information by Logical Outcomes Canada, that was reviewed and audited by AVAINTCON Consulting.

Revision History

Version	Section	Description	Author	Date
1.0			Robert Woodlock	
1.1			Robert Woodlock	2014-06-15
2.0		Final Release	Robert Woodlock	2014-07-22

Document Sign-off

Role	Name	Signature	Date
Author	Robert Woodlock – AVAINTCON Consulting		
Project Sponsor	Gillian Kerr – President – LogicalOutcomes		

Table of Contents

PIPEDA Report: LogicalOutcomes Canada

1 WHAT WE EXAMINED

LogicalOutcomes Canada ('LogicalOutcomes') is a Canadian not-for-profit organization that aims to improve the effectiveness of human services work and social policy by providing expertise and systems at a low cost, while building capacity and sustainability. They provide:

- expertise to help organizations work strategically
- tools to document impacts, communicate effectiveness and generate funding
- systems that are easy to implement and require minimal effort to keep running
- research on the impacts of programs on users and stakeholders
- training to build engagement and capacity to keep it all going.

This requires the collection and use of business and personal

- Names
- Addresses
- Postal Codes
- Phone numbers
- Email Addresses
- Responses to surveys and interviews via online, telephone and/or face-to-face contacts

We looked at how this information is managed, with a particular focus on how LogicalOutcomes assigns and monitors access to this information internally. Our audit examination was conducted between February 1st, 2014 and July 1st, 2014. During the audit we reviewed the way that LogicalOutcomes assigned privacy responsibilities, manages privacy risks and ensures compliance with the Privacy Act. We examined for personal information management policies, procedures, training materials, privacy impact assessments, breach investigations, internal audits and security reviews. We also reviewed information technology security, access to electronic systems and the monitoring of employees who access the data.

2 WHY THIS ISSUE IS IMPORTANT

LogicalOutcomes collects data in the process of carrying out stakeholder consultations and program evaluations. In either of these activities, project files may contain highly sensitive health and personal information. Project funders, stakeholders and service users expect that LogicalOutcomes is vigilant in ensuring that all necessary steps are taken to protect their personal information from inappropriate access, use or disclosure. Privacy breaches could potentially have a serious impact on the individuals affected in the form of stigmatization and/or personal embarrassment. Privacy breaches could also tarnish the LogicalOutcome Canada's reputation as a trusted custodian of Canadians' sensitive personal information.

3 WHAT WE FOUND

LogicalOutcomes has a culture of security and confidentiality through its integrity framework, policies, training, awareness and other initiatives. To date there have been no known privacy breaches involving the inappropriate access to personal information. In our opinion, the risk of breaches are low due to the small size of their organization, and their use of brand-name cloud solution offerings. Their weaknesses could grow as the organization expands, but LogicalOutcomes senior management has a clear dedication on external third party audits to ensure that personal information is protected from inappropriate internal or external access.

Findings:

a) LogicalOutcomes has not baselined their technology landscape for a 12 month period. Their technology solutions have changed on a quarterly basis, but this is typical with many new companies.

b) Privacy Impact Assessments are not always performed prior to the implementation of technology changes affecting personal information. This risk is lowered by using brand-name cloud services.

c) Threat and Risk Assessments are not completed for any information technology systems that process client information, which may result in undetected weaknesses.

d) The effectiveness of the LogicalOutcomes controls to detect and prevent inappropriate employee access and use of personal information is limited by its lack of an automated tool to identify and flag potentially inappropriate accesses and by certain gaps in the collection of audit trails on their systems.

e) LogicalOutcomes has made great progress to strengthen its privacy, security policies and procedures, and to communicate its expectations to employees/consultants about the safeguarding of personal information. LogicalOutcomes plans are also underway to improve access rights management and to more closely monitor employee access to clinical information. The observations and recommendations in this report are intended to enhance their personal information handling practices—and by extension, mitigate the risk of unauthorized access, use or disclosure of personal information. LogicalOutcomes has responded to our audit findings and its management responses follow each report recommendation

4 FOCUS OF THE AUDIT

The audit focused on employees' and consultants' electronic access to personal information. The audit objective was to determine whether LogicalOutcomes has appropriate controls and safeguards in place to protect personal information, and whether its policies, processes, procedures and practices comply with the fair information practices as described in sections 4 through 8 of the Privacy Act.

Observations and Recommendations

1. Our audit observations and recommendations are organized in four categories:
    a. privacy management and accountability;
    b. information technology security and governance;
    c. employee access and monitoring; and
    d. privacy breaches.
2. To meet the obligations of the Privacy Act, an organization must establish accountability for its compliance with the law. Our past audits of corporations and institutions have shown that when accountability is not clearly defined, gaps exist in the coordination and implementation of privacy related responsibilities. Those accountability gaps can place personal information at risk.

5 ABOUT THE AUDIT

Objective

The objective was to assess whether LogicalOutcomes has implemented adequate controls to protect personal information about its customers (including personal information that resides on returned data storage devices), and whether its policies, processes and practices for managing such information comply with the privacy principles listed in Schedule 1 of PIPEDA.

Criteria

We expected LogicalOutcomes to have implemented policies and processes that comply with the requirements of the collection, consent, use, disclosure and retention principles established under Schedule 1 of PIPEDA (Appendix B). Specifically, PIPEDA requires that:

- the purpose of collection of personal information be identified at or before the time of collection;

- consent of the individual be obtained prior to collection, use or disclosure of personal information;
- the collection of personal information be limited to that which is necessary for the purposes identified by the organization;
- personal information be used and/or disclosed only for the purposes for which it was collected, except with the consent of the individual or as required by law; and,
- personal information be retained only as long as necessary.

As per the requirements of the Safeguards Principle under PIPEDA, LogicalOutcomes is required to have appropriate measures in place to protect the personal information under its control.

Finally, in accordance with the Accountability and Openness Principles under PIPEDA, LogicalOutcomes is required to:

- define roles and assign responsibilities for privacy compliance throughout the organization;
- implement policies and procedures that give effect to the principles listed in Schedule 1 of the *Act*; including staff training; and,
- make readily available specific information about it policies and procedures relating to the management of personal information.

Scope and approach

The audit commenced with a survey of Logical Outcomes' personal information management practices. This included discussions with officials at LogicalOutcomes. A purposive sample strategy was used to establish the audit program. Audit evidence was obtained through various means, generally involving discussions, interviews and information obtained through correspondence. We also reviewed any policies, procedures, agreements, process-flow documents, training materials and IT system access controls.

The audit work was substantially completed on May 21, 2014.

Standards

The audit was conducted in accordance with the legislative mandate, policies and practices of the Office of the Privacy Commissioner, and followed the spirit of the audit standards recommended by the Canadian Institute of Chartered Accountants.

Audit team

Certified Information Systems Security Consultant: Robert Woodlock

6 Appendix A – Recommendations and Responses

1. **Include privacy specific compliance reviews as part of its internal audit program.**
    a. **LogicalOutcomes' response:**
    - The company agrees with the recommendation.
    - The company has made changes to its loss prevention audit checklist to address information storage, collection, retention and disposal of personal information and other privacy related items in more depth.
    - The company has established a program of yearly security audit with a 3rd party security vendor. The company has adopted a Code of Ethics – the Tri-Council Policy [http://www.pre.ethics.gc.ca/pdf/eng/tcps2/TCPS_2_FINAL_Web.pdf] which reinforces privacy protection priorities.

2. **LogicalOutcomes should make clients aware of all potential uses and disclosures of their personal information, including any data transfers to foreign jurisdictions.**
    a. **LogicalOutcomes' response:**

- The company agrees with the recommendation.
- The company will make appropriate changes to its corporate privacy policy by August 15, 2014.

3. **LogicalOutcomes should ensure that paper based personal information is stored in locked cabinets or secured areas, as required by its policy.**
    a. **LogicalOutcomes' response:**
- The company agrees with the recommendation.
- The company will communicate and hereafter will continue to enforce its policies with respect to personal information storage and has included this matter in its internal audit procedures.

4. **LogicalOutcomes should ensure that staff is reminded of the importance of using secure methods to destroy customer data.**
    a. **LogicalOutcomes' response:**
- The company agrees with the recommendation.
- The company will communicate and hereafter will continue to enforce its policies with respect to personal information storage and has included this matter in its internal audit procedures.

5. **LogicalOutcomes should ensure that employees have unique system access credentials to facilitate user accountability and mitigate the risk of unauthorized access to customer data.**
    a. **LogicalOutcomes' response:**
- The company agrees with the recommendation.
- The company continues to use off-the-shelf practical systems to access security solutions and its current cloud platform enables individual secured access.

7 Appendix B – Principles under Schedule 1 of PIPEDA considered during this audit

Principle 1 — Accountability

1. An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

3. The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

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

Organizations shall implement policies and practices to give effect to the principles, including

a) implementing procedures to protect personal information;

b) establishing procedures to receive and respond to complaints and inquiries;

c) training staff and communicating to staff information about the organization's policies and practices; and

d) developing information to explain the organization's policies and procedures.

Principle 2 — Identifying Purposes

1. The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

2. The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle and the Individual Access principle.

3. Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfill these purposes. The Limiting Collection principle requires an organization to collect only that information necessary for the purposes that have been identified.

4. The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

5. When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle.

6. Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

7. This principle is linked closely to the Limiting Collection principle (Clause 4.4) and the Limiting Use, Disclosure, and Retention principle.

Principle 3 — Consent

1. The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

2. Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

3. The principle requires “knowledge and consent”. Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

4. An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes.

5. The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

6. In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual’s name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual’s request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

7. The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

Individuals can give consent in many ways. For example:

a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;

b) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;

c) consent may be given orally when information is collected over the telephone; or

d) consent may be given at the time that individuals use a product or service.

8. An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

Principle 4 — Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

1. Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfill the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle.

2. The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

3. This principle is linked closely to the Identifying Purposes principle and the Consent principle .

Principle 5 — Limiting Use, Disclosure, and Retention

Personal information shall 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. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

1. Organizations using personal information for a new purpose shall document this purpose.

2. Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

3. Personal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

4. This principle is closely linked to the Consent principle, the Identifying Purposes principle, and the Individual Access principle.

Principle 6 — Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

1. The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

2. The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

3. The methods of protection should include

a) physical measures, for example, locked filing cabinets and restricted access to offices;

b) organizational measures, for example, security clearances and limiting access on a “need-to-know” basis; and

c) technological measures, for example, the use of passwords and encryption.

Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

Principle 7 — Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

The information made available shall include

a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;

b) the means of gaining access to personal information held by the organization;

c) a description of the type of personal information held by the organization, including a general account of its use;

d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and

e) what personal information is made available to related organizations (e.g., subsidiaries).

An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.