CAN/DGSI 100-11:2025
NATIONAL STANDARD OF CANADA

First Edition
2025-05

Data governance – Part 11: Delivery of community and human services

03.100.02; 03.100.40; 35.020; 35.030

- Page left intentionally blank -

Table of Contents

- Page left intentionally blank -

Foreword

The Digital Governance Standards Institute (DGSI) develops digital technology governance standards fit for global use. The Institute works with experts, as well as national and global partners and the public to develop national standards that reduce risk to Canadians and Canadian organisations adopting and using innovative digital technologies in today's digital economy.

DGSI standards are developed in accordance with the *Requirements & Guidance – Accreditation of Standards Development Organisations*, 2019-06-13, established by the Standards Council of Canada (SCC).

Attention is drawn to the possibility that some of the elements of this Standard may be the subject of patent rights. DGSI shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of this Standard are included in the Introduction.

For further information about DGSI, please contact:

Digital Governance Standards Institute
500-1000 Innovation Dr.
Ottawa, ON K2K 3E7
www.dgc-cgn.org

A National Standard of Canada is a standard developed by a Standards Council of Canada (SCC) accredited Standards Development Organisation, in compliance with requirements and guidance set out by SCC. More information on National Standards of Canada can be found at www.scc.ca.

SCC is a Crown corporation within the portfolio of Innovation, Science and Economic Development (ISED) Canada. With the goal of enhancing Canada's economic competitiveness and social well-being, SCC leads and facilitates the development and use of national and international standards. SCC also coordinates Canadian participation in standards development, and identifies strategies to advance Canadian standardization efforts.

Accreditation services are provided by SCC to various customers, including product certifiers, testing laboratories, and standards development organisations. A list of SCC programs and accredited bodies is publicly available at www.scc.ca.

- Page left intentionally blank -

Introduction

This is the First Edition of CAN/DGSI 100-11:2025, Data Governance – Part 11: Delivery of Community and Human Services.

CAN/DGSI 100-11:2025 was prepared by the DGSI Technical Committee 1 (TC 1) on Data Governance, comprised of over 260 thought leaders and experts in data governance and related subjects. This Standard was approved by a Technical Committee formed balloting group, comprised of 4 producers, 3 government / regulator / policymakers, 4 users, and 4 general interests.

All units of measurement expressed in this Standard are in SI units using the International system (SI).

This Standard is subject to technical committee review beginning no later than two years from the date of publication. The completion of the review may result in a new edition, revision, reaffirmation or withdrawal of the Standard.

The intended primary application of this Standard is stated in its scope. It is important to note that it remains the responsibility of the user of the Standard to judge its suitability for a particular application.

This Standard is intended to be used for conformity assessment.

03.100.02; 03.100.40; 35.020; 35.030

CETTE NORME NATIONALE DU CANADA EST DISPONIBLE EN VERSIONS FRANÇAISE ET ANGLAISE

- Page left intentionally blank -

Context

This Standard is supported by a volunteer Technical Committee and an eight-member drafting team comprised of volunteers with subject matter expertise and interest from across the Canadian nonprofit sector, including organisations such as the Ontario Nonprofit Network (ONN), the Ontario Trillium Foundation (OTF), Common Approach to Impact Measurement, Canadian Mental Health Association (CMHA) Toronto, New Brunswick Institute for Research, Data and Training (NB-IRDT), and the Canadian Centre for Nonprofit Digital Resilience (CCNDR). The drafting team co-wrote the Standard while the Technical Committee reviewed and provided feedback on the Standard before the DGSI posted it for public review, committee approval, ratification and publication.

This Standard is relevant to organisations that deliver community and human service programming, including programming funded by a third party, to enable them to safeguard data *privacy*. Data *privacy* practices require organisations to shift their understanding of data *privacy* from an administrative or an operational task to understanding it as a fundamental obligation including providing data *privacy* training to volunteers tailored to their specific tasks and responsibilities. Third party funders need to consider how to provide the necessary resources to nonprofits when mandating the collection of *personal information* as a condition of funding.

Data Governance and the Importance of Standards

Data governance in community and human services serves several purposes. It is key to keeping an organisation's data usable, accessible and protected. It clarifies who is responsible for data in an organisation and requires organisations to establish practices or policies for every stage of *the data life cycle*. It considers the organisational relationship to data, sets principles or values aligned to the organisation's mission and mandate, and distributes data-related responsibilities to appropriate staff or volunteers. Governance is the central pillar of any data strategy.

Standards in data governance are critical to organizing, documenting, and representing (both explaining and *classifying* meta-data) data so it can be better used and shared. It can range from simple decisions on data entry to more complex decisions around anonymizing a particular data set. Data governance standards are most effective when they are used collectively, as they can enable critical conversations and clarification on definitions, especially in situations when subsectors may have their own acronyms. Aligning with the same standards across organisations can help compare similar programming, identify cost-saving or cost-effective practices, or link their data to other data sets for additional insights.

As a tool for learning, this Standard reduces barriers to the work that must be done collectively as a sector. An understanding of *equity*, particularly past and present harms caused by how data is governed, collected, accessed, used, shared and stored was central to developing this Standard. The Technical Committee recognizes that these harms have been disproportionately experienced by Indigenous, Black and *racialized* communities. It is the hope of the Technical Committee that through the creation of this standard, other data initiatives, such as the First Nations data principles of ownership, control, access and possession (OCAP®) and the City of Toronto's Black Community Data Governance Framework, can

be complemented to support data sovereignty and *equity*.

Data Governance for Artificial Intelligence

Robust data governance frameworks form a solid foundation for any organisation's AI governance program before they use, develop or deploy artificial intelligence systems and tools. This includes clearly defined policies, controls and procedures for data collection, access, use, sharing and storage of *personal information*; the implementation of security measures to protect personal, health, and business confidential information, and compliance with cybersecurity protocols. Organisations must also ensure that their data governance practices align with relevant Canadian laws and regulations, such as the Personal Information Protection and Electronic Documents Act (PIPEDA), provincial health information *privacy* legislation, intellectual property laws, the Canadian Human Rights Act, and related provincial or territorial legislation. This ensures that organisations handle data in an ethical, secure, and compliant manner so that they can responsibly and effectively deploy generative AI in ways that can advance their missions and safely serve their communities.

Data Monetization

In the context of data governance, data monetization refers to using data as a strategic asset to generate financial returns or improve operational effectiveness, thereby freeing organisational capacity to be redirected to mission-focused activities. This involves the data-insight-action process (Wixom, Beath, & Owens, 2023) where data is analyzed to derive insights that inform strategic decisions or actions. Revenue can be generated through data insights, data sharing, licensing, or selling anonymized data sets.

However, data monetization is not just about financial gains. Ethical considerations —ensuring that all data monetization activities align with the mission, *equity* commitments and core values of the organisation, and comply with relevant laws and regulations as well as the consent of individuals to whom the data belongs when appropriate— are at the heart of this process. While organisational investments in data infrastructure and capabilities can be costly and increase annual operating costs, these investments are not merely expenses but strategic moves that can create measurable, long-term, sustainable value.

It is crucial to assess what value an organisation's data initiatives can most effectively create—generating actionable insights, enhancing operational efficiency, improving service delivery, or fostering innovation—to focus efforts where they can strategically generate the most impact. In this way, through ethical and effective data governance, organisations can fund more programs, improve services, and build partnerships that enhance their capabilities and community impact.

Data governance – Part 11: Delivery of community and human services

1 Scope

This document specifies minimum requirements for the responsible and *privacy*-preserving collection, access, use, sharing and storage of *personal information* by organisations delivering community and human services. This Standard serves as a guide to help nonprofit organisations and funders engage with their data in ethical and equitable ways and to advance the culture of data collection, access, use, sharing storage in the sector.

This document is also applicable to nonprofit organisations that are typically small to medium-sized organisations that work within the constraints of smaller teams and a larger breadth of responsibilities in job roles.

Considerations are given to:

- relevant guidelines and practices for *data equity*;
- client/beneficiary and donor data;
- data governance and management practices;
- *privacy* regulations and other applicable legislation;
- relevant ethical guidelines and practices; and
- requirements for service providers, funders, and technology vendors.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

Black Health *Equity* Working Group, EGAP Framework.

City of Toronto, Black Community Data Governance Framework.

First Nations Information Governance Centre, First Nations Principles of OCAP®.

Ontario Nonprofit Network, A Framework for Nonprofit Data Strategies.

The National Association of Friendship Centres, National Data Strategy.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply:

confidentiality
The ability to protect and control *sensitive data* from access by unauthorized people.

[SOURCE: CAN/DGSI 104:2021 / Rev 1: 2024. Modified]

data breach
A cyber security incident wherein there is theft of, loss of, or unauthorized collection, use or disclosure of, *sensitive*, protected or confidential information.

[SOURCE: CAN/DGSI 104:2021 / Rev 1: 2024]

data classification
A scheme that provides the basis for managing access to, and protection of, data assets.

[SOURCE: International Association of Privacy Professionals' Glossary of Privacy Terms]

data collector
Person or entity that collects data.

data controller
The party that, alone or jointly with others, determines the purposes and means of the processing of personal data. The actual processing may be delegated to another party, called the *data processor*. The controller is responsible for the lawfulness of the processing, for the protection of the data, and respecting the rights of the *data subject*. The controller is also the entity that receives requests from *data subjects* to exercise their rights.

[SOURCE: European Data Protection Supervisor's Glossary of Data Protection Terms]

data equity
Principles and practices to guide data work through a lens of diversity, justice, *equity* and inclusivity.

[SOURCE: Ontario Nonprofit Network's A Framework for Nonprofit Data Strategies]

data life cycle
The flow of information through a life cycle from creation to final disposition.

[SOURCE: International Association of Privacy Professionals' Glossary of Privacy Terms]

data owner
Person or entity responsible for the governance of particular organisational data sets.

data processor
A natural or legal person (other than an employee of the controller), public authority, agency or other body which processes personal data on behalf of the controller. An organization can be both a controller and a processor at the same time, depending on the function the organization is performing.

[SOURCE: International Association of Privacy Professionals' Glossary of Privacy Terms]

data security
The processes, actions, policies, regulatory requirements, responses, and procedures applied, communicated, adhered to, agreed to, and monitored, to protect the *confidentiality* and integrity of information.

NOTE: In many cases, the application of these protection measures requires adherence to national and/or international laws.

[SOURCE: CAN/DGSI 100-2: 2022 / Rev 1: 2024]

data sensitivity
How data can have potentially harmful effects in the event of disclosure or misuse.

[SOURCE: CAN/DGSI 117:2023]

data stewardship
Collecting, retaining, using, destroying and disclosing data, and as part of that, making decisions about who has access to data, for what purpose and to whose benefit.

[SOURCE: Open Data Institute, applying new models of data stewardship to health and care data (modified)]

data subject
Person or entity whose data is being processed.

[SOURCE: CAN/DGSI 100-2: 2022 / Rev 1: 2024]

data user
Person or entity that can use and interact with the data.

encryption
Converting information from one form to another to hide its content and prevent unauthorized access.

[SOURCE: Canadian Centre for Cyber Security]

equity
The removal of systemic barriers (e.g., unconscious bias, discrimination, racism, sexism, ableism, homophobia, etc.), enabling all individuals to have equitable opportunity to access and benefit from the program

[SOURCE: Government of Canada's Best Practices in Equity, Diversity and Inclusion in Research Practice and Design]

personal information
Information about an identifiable person.

[SOURCE: CAN/DGSI 103-1:2023 (R2024)]

privacy
The right of individuals to determine for themselves what information about them is collected, accessed, used, shared and stored.

[SOURCE: Privacy and Freedom, Alan F. Westin, New York: Atheneum, 1967]

racialized
A person or group of people categorized according to ethnic or racial characteristics and subjected to discrimination on that basis.

[SOURCE: Government of Canada's Guide on Equity, Diversity and Inclusion Terminology]

4 Governance and Oversight

4.1 Context

4.1.1 This section specifies baseline requirements for data governance principles that should be followed across all stages of the *data life cycle*. These principles apply to organisations. *Data collectors, data controllers*, *data users*, and *data processors* must acknowledge that data is not inherently neutral. Data can contain biases and reflect the perspectives and values of those who collect, analyse and interpret it.

4.2 Accountability and Monitoring

4.2.1 The organisation shall develop a data governance plan.

NOTE: The data governance plan may be part of other governance plans that exist or are being developed.

4.2.2 The organisation shall designate a role responsible for overseeing the data governance plan and ensuring compliance.

4.2.3 Regular audits shall be conducted to monitor the compliance and effectiveness of the data governance plan.

4.3 Informed Consent

4.3.1 The organisation shall ensure that informed consent obtained from users of human and social services prior to data collection identifies all possible stages of the *data life cycle*.

4.3.2 Informed consent may include but is not limited to the following areas:

a) how and in what form that data will be shared.

b) whether identifiable data will be shared.

c) for what purposes the data will be accessed and used.

d) the role the *data owner* has in any data sharing.

e) making clear to the *data subjects* at what point in time they have the right to withdraw their data from any sharing.

4.3.3 In the event that informed consent is not able to be obtained from the *data subject*, the organisation shall refer to appropriate *privacy* legislation.

4.4 Data Equity

4.4.1 The organisation shall recognize and respect Indigenous data sovereignty and data governance for Black peoples.

4.4.2 Recognizing the principle of data sovereignty, where data laws are jurisdiction-specific, and ensuring equitable data treatment across all users, regardless of location. To further uphold user rights, the principle of 'Data Self-Sovereignty by Design' will be integrated throughout the development and implementation of this [product/service], as outlined in section 4.4.1.

4.4.3 The organisation should adhere to data governance frameworks for Indigenous and Black peoples.

NOTE: Examples of frameworks include the First Nations data principles of ownership, control, access and possession (OCAP®) and the National Data Strategy for Friendship Centres when working with Indigenous communities, as well as the City of Toronto’s Black Community Data Governance Framework, and the Black Health *Equity* Working Group’s Engagement, Governance, Access and Protection (EGAP) Framework.

4.4.4 *Data collectors* should adhere to *data equity* principles and include *data equity* strategies in their data governance plan. *Data equity* strategies should:

a) Seek to address the needs of racialised and marginalised groups, with particular attention to Black and Indigenous peoples, in relation to all points of the *data life cycle*.

b) Empower racialised and marginalised groups to participate in data governance processes.

c) Ensure that the organisation's data governance practices do not perpetuate biases or lead to discriminatory outcomes.

d) Engage communities using *equity*-based approaches to data governance that build trust and minimise harm.

e) Examine the social and historical context to identify the root causes of disparities, inform data collection and use, and develop data-driven solutions.

f) Ensure data visualisations promote inclusion and awareness across culturally, linguistically, and racially diverse audiences.

g) Seek agreement from *data subjects* on the interpretation of their data sets.

h) Ensure data is disaggregated to help analyse disparities, monitor progress, and guide action.

i) Question their default methods, assumptions, and dominant culture narratives for data collection and analysis and triangulate quantitative data with other sources. (Gonzalez, et al., 2024).

5 Data Collection

5.1 Context

5.1.1 This section specifies the principles and requirements for the collection of data. These principles and requirements apply to *data collectors*, *data controllers*, *data stewards*, *data users*, and *data processors* and outline their responsibilities to *data subjects*.

5.2 Permission to Collect

5.2.1 The organisation shall document the specific objectives for collecting, processing, and retaining data.

5.2.2 Data collection shall comply with all applicable laws and regulations.

5.2.3 The organisation shall have a policy that governs data collection as part of its data governance plan.

5.2.4 The organisation shall obtain consent, express or implied, voluntarily from all *data subjects* before data collection according to the purpose and types of data collected.

5.2.5 The consent process shall include clear, understandable information about the purpose, scope and use of the collected data.

5.2.6 The organisation shall make clearly available to the *data subject* its process to withdraw consent at any time during and after the collection process or at what point data can no longer be withdrawn. This process may necessitate the deletion or modification of the data collected.

5.3 Data Quality and Integrity

5.3.1 The organisation shall provide clear information about data governance practices that is accessible to *data subjects* at the time of collection and to all interested parties.

5.3.2 Data collected shall conform to data quality principles of completeness, accuracy, recency, timeliness, and integrity to the best of the ability of the organization.

5.4 Data Minimisation

5.4.1 *Data controllers* should limit the collection of *personal information* to what is directly relevant and necessary to accomplish the specified purpose of the data collection.

5.4.2 *Data controllers* should retain the data only for as long as is necessary to fulfil that purpose.

5.4.3 Data shall not be used or disclosed for purposes other than those for which it was collected, except with express consent or as required by law.

5.4.4 Data retention periods shall be defined based on the purpose of data collection and legal requirements, after which data shall be securely destroyed.

6 Data Storage

6.1 Context

6.1.1 This section specifies the principles and requirements for secure storage of data collected by human and social service organisations. These principles and requirements apply to *data collectors*, *data controllers*, *data users*, and *data processors* and outline their responsibilities to *data subjects*. Appropriate data storage is crucial for maintaining the integrity, *confidentiality*, and availability of information, thereby ensuring that data is protected from unauthorized access, alteration, loss, or destruction. The onus lies on the organisation.

6.1.2 Data residency requirements should be carefully considered and regularly evaluated, balancing potential benefits with potential risks. Examples include but are not limited to personal *privacy*, public safety, domestic and national security, hindering innovation, and limiting access to services, etc.

6.2 Data Protection and Security

6.2.1 The organisation shall have a policy that governs data storage as part of its data governance plan.

6.2.2 *Data security* measures shall include technical, physical and organisational safeguards appropriate to the sensitivity of the data.

6.2.3 The role, committee, or working group responsible for organisational data protection and *data security* shall engage in ongoing *data security* training.

6.3 Data Storage

6.3.1 The organisation shall determine a data storage solution (e.g physical, cloud, on-premise, hybrid) that best protects and secures data collected.

6.3.2 Physical data shall be stored in a secure location with limited access.

6.3.3 The organisation shall document as part of its data storage policy where cloud or on-premise data is stored and what data protection laws are applicable to those locations.

6.3.4 Data shall be classified based on its *sensitivity* level.

6.3.5 The organisation shall determine the appropriate use of personal devices to access data.

6.4 Technical Safeguards

6.4.1 All data, both in transit and at rest, shall be encrypted using industry-standard e*ncryption* protocols.

6.4.2 Access to data shall be role-based. Only authorized personnel with a legitimate business need shall have access to *sensitive data*.

NOTE: *Sensitive data* is typically a category of information where harm and injury starts to exceed a certain threshold.

6.4.3 Multi-factor authentication (MFA) shall be implemented for accessing systems that store or process *sensitive data*.

6.4.4 The organisation shall conduct regular *data security* audits and vulnerability assessments to identify and mitigate potential risks.

6.4.5 The organisation shall monitor and log system access and data transactions, to detect and respond to any unauthorized activities promptly.

6.5 Backup and Recovery

6.5.1 The organisation should store data in multiple different locations (e.g. physical, cloud, on-premises, hybrid).

6.5.2 The organisation shall implement an automated backup solution that is tested regularly.

6.5.3 The organisation shall ensure regular software updates.

6.6 Retention and Archiving

6.6.1 The organisation shall implement a data retention policy for how long various kinds of data will be kept and eventually destroyed. The policy shall consist of any requirements found in appropriate legislation and records/certificates of destruction.

6.6.2 Data shall be retained for only as long as necessary to complete the task for which it was collected.

7 Data Access and Use

7.1 Context

7.1.1 This section specifies the actions to be taken with respect to the secure access and use of personal data and or personal health data held in custody. *Data users* are accountable for their actions with respect to access and use of personal data. Accountability can be acknowledged through administrative safeguards and best practices such as the use of *confidentiality* agreements and attestations to *privacy* policy awareness.

7.2 General

7.2.1 The organisation shall have a policy that governs data access and use as part of its data governance plan.

7.2.2 The organisation shall maintain transparency in data practices. This may include communicating about how the data is used and access to notifying *data owners* of a *data breach*.

7.2.3 *Data users* shall receive data *privacy* training prior to any data collection, access, use, sharing or storage and on a continuing basis to reinforce *privacy* best practices.

NOTE: The Office of the Privacy Commissioner of Canada provides data *privacy* training tools.

7.2.4 Training shall be appropriate to the data being accessed and used and updated regularly to help ensure compliance with legislation and best practices.

7.2.5 Training shall include appropriate data incident or *data breach* identification and response.

7.2.6 Access to data shall be limited to the minimum amount of data necessary to complete the purpose for its access. A roles-based approach to user access and use permissions may be applied.

7.2.7 Data shall be accessed and used in the most de-identified format possible to complete the task.

7.2.8 Access and use shall only be for the purposes for which the data were collected and the consent of individuals obtained.

7.2.9 All new or additional purposes for access and usage shall require the consent or reconsent of individuals to whom the data pertains.

7.2.10 A mechanism shall be in place to allow for data access for the purposes of correction and accuracy at the request of the individual to whom the data pertains.

NOTE: There may be times where this is not possible or feasible, such as anonymous surveys or anywhere that the response can't be tied to the individual person.

7.2.11 A mechanism shall be in place to facilitate secure access should data access be required under an Act of Legislature.

7.2.12 User access and use permissions shall be removed when roles are vacated.

7.2.13 The organisation shall ensure their data interpretation methods produce accurate and reliable results that align with data collection objectives.

8 Data Sharing and Publishing

8.1 Context

8.1.1 This section specifies the principles and requirements for sharing the data collected by human and social service organisations. Sharing data may be necessary for the users and providers of human and social services, helping to inform and guide current and future programming. A guiding principle throughout this section is the recognition that users of human and social services have the right to know how their data will be used and shared, and the right to refuse that sharing of their data at any point after collection.

8.2 General

8.2.1 The organisation shall have a policy that governs data sharing and publishing as part of its data governance plan.

8.2.2 The organisation shall identify the consequences of their data sharing on the users of human and social services.

8.2.3 The organisation shall minimise the extent of data sharing to only that which might be required for the purposes defined above, balancing the *privacy* expectations of the individuals or organisations whose data may be shared with any applicable federal laws, regulations, policies and guidelines.

8.2.4 The organisation shall identify what data will be shared and who that data will be shared with, in what format and how the data shall be shared.

8.2.5 De-identification of data shall be standard practice when sharing data, unless otherwise indicated or required. In cases where identifying data is required to be shared (for example in the sharing of identifying information required for the provision of a further service), applicable laws, regulations, policies and guidelines will apply.

8.2.6 The organisation shall ensure that data are only shared through secure channels of communication using robust security measures and meet all applicable laws, regulations, policies and guidelines for communication of human and social services data.

8.2.7 The organisation shall implement protocols, formats and vocabularies that ensure data can be effectively exchanged and used across different systems and software without alteration of meaning or intent.

8.3 Data Sharing Agreements

8.3.1 The organisation shall identify any third parties with which data will be shared.

8.3.2 The organisation shall enter into data sharing agreements prior to sharing any data with a third party.

8.3.3 The organisation shall ensure there is an appointed role responsible for ensuring all the terms of the data sharing agreements are enforced.

8.3.4 The data sharing agreements shall define the terms and conditions around data sharing, how the data will be shared, and for what purposes the data may be used and shared further.

8.3.5 The data sharing agreements shall specify how the *privacy* of the owners of the data will be maintained, how the data will be securely retained and how data may be further shared.

8.3.6 The data sharing agreements shall specify where, how and how long the data shared will be stored by any third party.

8.3.7 The data sharing agreements shall identify when the data will be destroyed and any requirements for certification of destruction.

Bibliography

[1] European Data Protection Supervisor. (2024). *Glossary*. Retrieved April 20, 2024, from https://www.edps.europa.eu/data-protection/data-protection/glossary_en

[2] Gonzalez, N., Alberty, E., Brockman, S., Nguyen, T., Johnson, M., Bond, S., . . . Mean, S. F. (2024, April 20). *Education-to-Workforce indicator framework: Using data to promote equity and economic security for all.* Retrieved July 19, 2024, from https://www.mathematica.org/publications/education-to-workforce-indicator-framework-using-data-to-promote-equity-and-economic-security

[3] International Association of Privacy Professionals. (2024). *Glossary of Privacy Terms.* Retrieved July 19, 2024, from https://iapp.org/resources/glossary/

[4] Law for Non-Profits. (2024). *Top Tips for Maintaining Data Privacy*. Retrieved July 19, 2024, from https://lawfornonprofits.ca/blog/top-tips-maintaining-data-privacy

[5] NTEN, (2021). *Data policies your nonprofit needs.* Retrieved July 19, 2024, from https://word.nten.org/wp-content/uploads/2021/10/Data-Policies-Your-Nonprofit-Needs.pdf

[6] Office of the Privacy Commissioner of Canada. (2019, May 31). *PIPEDA Fair Information principles.* Retrieved April 20, 2024, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

[7] Ontario Nonprofit Network (ONN). (2023). *A Framework for Nonprofit Data Strategies.* Retrieved April 20, 2024, from https://theonn.ca/publication/deal-framework/

[8] Own Company. (2023, August 18). What Every Nonprofit's Data Protection Solution Should Include. Retrieved July 19, 2024, from https://www.owndata.com/blog/what-every-nonprofits-data-protection-solution-should-include

[9] The First Nations Information Governance Centre. (2023, July 25). *The First Nations Principles of OCAP®*. Retrieved April 20, 2024, from https://fnigc.ca/ocap-training/

[10] Wixom, B. H., Beath, C. M., & Owens, L. (2023). *Data Is Everybody's Business: The Fundamentals of Data Monetization.* Cambridge, Massachusetts, USA: The MIT Press. Retrieved May 12, 2024