WORKING DOCUMENT

Data Governance Framework of Montréal in Common

TOWARDS A MORE RESPONSIBLE, EFFECTIVE, AND COLLABORATIVE DATA GOVERNANCE

YOU WILL FIND... **An interpretation of the principles of** the Montréal Digital Data Charter

Reasons for operationalizing each principle

Logical links between principles

A list of tactics (concrete actions) to deploy the Charter principles

VERSION Version 1.0, January 2022

Montréal en commun

NordOuvert

The Data Governance Framework is a complementary document to the tools developed by the Data Governance Workstream of Montréal in common. To learn more about our work, we invite you to consult the Data Governance Workstream.

Links to other data governance tools

- Data Governance Journey User Guide
- Data Governance Framework
- Decision diagram of a data use case (in FR)
- Data Governance Self-Assessment Tool (in FR)
- Appendices (in FR)

Working document: This tool is a working document. This means two things: 1) it is an intermediate version, in this case the first one, and 2) we are counting on your constructive feedback to improve the tool for the next version. Any comments? An idea? Please send them to us by filling in this form.

You can quote this tool as follows: *Open North. Data Governance Framework for Montréal in Common: Towards a more responsible, effective, and collaborative data governance. Open North, 2022.*

Disclaimer: If you create an adaptation of this work, please add the following disclaimer with the attribution: This is an adaptation of an original work by Open North. The views and opinions expressed in the adaptation are the sole responsibility of the author and the adaptation is not endorsed by Open North.

Authors: Samuel Kohn, Lauriane Gorce, Marie Plamondon, Karine Saboui, Steve Coutts, Dominique Camps, Lucas Mesquita, Alexandre Cailhier

Introduction

Before reading this document, we invite you to read the Data Governance Journey User Guide! It will help you better understand the importance of consistent data governance as well as the proposed pathway. It also presents the tools developed to support you in your approach. Finally, the appendix contains a glossary and a bibliography.

Montréal in Common (MiC), the Montréal chapter of Canada's Smart Cities Challenge, is a local, multi-sectoral innovation community. It brings together organizations from the public sector, academia and the social economy to collaborate and experiment to find effective solutions to local problems. A human-centred approach, fostered by responsible and responsible governance, is at the heart of the program. Data and new technologies are harnessed only when appropriate, in a measured way, as a means to achieve the goals of the program and its 13 projects.

The MiC data landscape is very heterogeneous. As program partners, we use a variety of data types and technologies to support our activities and projects. However, we see a few common denominators in the ecosystem with respect to data use and governance. For example, we all seek to use data to reflect similar values: 1) make informed decisions; 2) drive innovation; 3) demonstrate project impact; 4) inform the public; and 5) ensure legal compliance and reliable accountability.

More generally, we are bound by a shared vision: to use data for the common good and to respect the principles of the City of Montréal's Digital Data Charter (hereafter *Charter*) in order to support the social inclusion and ecological transition movements.

The Montréal in Common data governance framework is a formal document that builds on the Charter principles to guide our innovation community towards more responsible, effective and collaborative data governance.

The data governance framework is divided into two main sections:

1. **Interpretation of the Charter principles**, adapted to the MiC context. For each principle, you will find its concrete definition, the reasons why it should be operationalized and its links with other principles.
2. **Tactics**, which are the concrete actions you need to take to comply with the Charter principles and move towards more responsible, effective and collaborative data governance.

The tactics documented in this first version of the framework will evolve based on new learning from the community of practice as well as the program's data governance capacity building program that will begin in early 2022. The tactics will also adapt, as needed, to the ever-changing legal, technical, technological, and social factors that influence data governance in the ecosystem.

The project is ambitious. The long-term goal is for the MiC community to have the capacity, skills and motivation to go after more advanced tactics, always in the spirit of continuous learning and improvement.

Embarking on the path of data governance, as with the path of socio-ecological transition, is not an easy one, but there are many lasting benefits for both Montréalers and MiC partners.

Table of content

The principles

The City of Montréal's Digital Data Charter brings together various principles, ensuring individual and collective human rights, while emphasizing the importance of coming together around a common societal project, through orientations regarding data operations and uses.

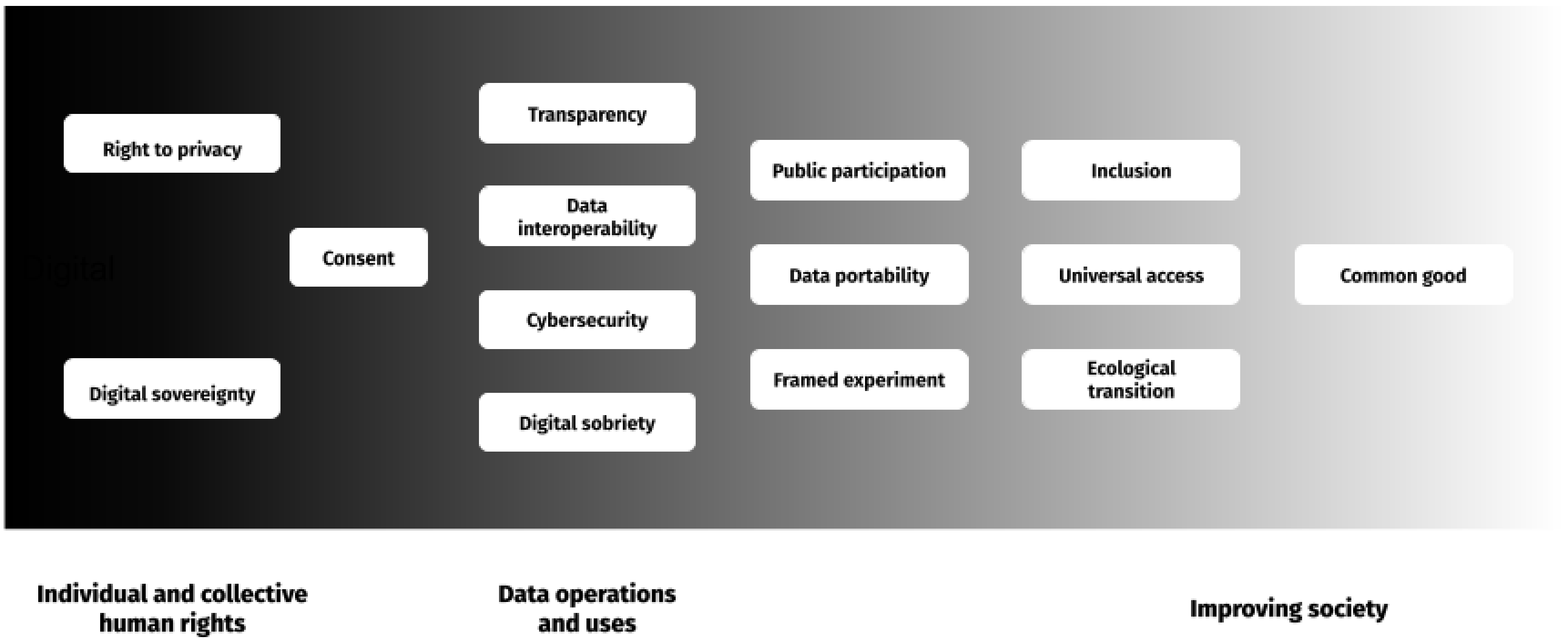


Figure 1: The principles of the City of Montréal's Digital Data Charter

Definition and relevance of each principle

The contextualization of the Charter principles is intended to lay the foundation for a shared language for the innovation community of Montréal in Common and beyond. For each principle, you will find its concrete definition[1] and the reasons why it should be operationalized.

RIGHT TO PRIVACY

The human right of an individual to control who has access to his or her personal data*[2] , when and under what circumstances, with the aim of preventing any intrusion into his or her privacy. The right to privacy is a gateway to other rights that are essential to a democracy (e.g. the rights to free speech, non-discrimination, dissent). Yet in the age of massive data, the risks of state and corporate surveillance are high and unrecognized. Individuals are increasingly discriminated against for the main reason that they are part of a group, whether they are aware of being part of that group or not (when they are categorized by algorithms in clusters*). When a person discloses their personal data, it enriches the information about all the groups they belong to. Therefore, it is important to move from the individual to the collective scale as well as to move from abstract concepts to a more robust understanding of the activities that threaten the privacy rights of individuals and communities, their risks, and their mitigation.

The right to privacy should not be confused with **data protection**, which refers to the means and tools (often legal) that regulate the management of personal data, whether the individual decides to make it public or keep it private (in which case data protection refers to the means and tools to enable an individual to exercise his or her right to privacy). In practice, data protection frameworks grant individuals (but not yet communities) technical rights over their data (information, access, rectification, deletion or right to be forgotten, portability...) and establish clear accountability systems and obligations for those who control or undertake data processing.

Reasons for operationalizing this principle

1. Beyond legal obligations, demonstrate your responsibility and good faith in the collection and management of data.
2. Provide better guarantees to individuals and organizations through your service offerings by collecting only the necessary data.
3. Establish decision-making processes that allow communities and individuals, as experts in their own lives, to identify the priorities and risks of potential data collection projects.

[1] Definition proposed by Open North based on a scan of the literature supplemented by exchanges with experts.
[2] All words marked with an asterisk are defined in the glossary.

DIGITAL SOVEREIGNTY

The ability or right of an individual or group to govern data based on a variety of factors, including their values, laws and customs. Individuals or groups whose digital data is collected and used must have a say in the governance of their data. The common thread in digital sovereignty is the need for stakeholders (governments, Indigenous peoples, individuals, social movements...) to control their data and data flows, to have their human rights respected, and to actively participate in data management and technology development.

Reasons for operationalizing this principle

1. Ensure that the needs, values, and rights of the groups whose data is collected are respected and accurately reflected by actively collaborating with them from all aspects of data management through the design, deployment, and use of data-driven technology.
2. Maintain close control of critical systems or data by the individuals, groups, or governments involved, for example, by not outsourcing their administration to a third party.

CONSENT

Consent occurs when an individual agrees to share some of his or her directly or indirectly identifiable data for a specific purpose. Consent in data sharing is often associated with a trade-off of data for a service. However, consent should not be used as a means of exchanging data for a service when the power relationship between the service provider and the person providing the data is asymmetric. Clear, free and informed consent is important because it ensures that individuals have control over their digital footprint. To ensure that consent is informed, digital literacy* must be strengthened, or else the individual does not truly understand what he or she is consenting to. The organization collecting the data must transparently inform the framework of the use of the data and obtain clear consent for such use.

Reasons for operationalizing this principle

1. Foster trusting relationships between parties who share their data and consume the data through consent mechanisms honored by both parties.
2. Demonstrate commitment to the individual's right to control their data through consent documents honored by both parties.

TRANSPARENCY

An approach that involves sharing and communicating data practices. Transparency includes sharing information about the intent behind the use of the data, the methods used to collect the data (including a rationale, if any, for why certain data are ignored), the changes or processes used to transform the data, and the methods of sharing. It can also include the publication of the data itself as open data. An important aspect of transparency is communication and its related tools used to disseminate methodologies about practices used.

Reasons for operationalizing this principle

1. Foster dialogue about the value of data between partners and the public.
2. Improve collaboration in the event of partnerships or opening of data because it improves the understanding of the context and history of shared datasets.
3. Build trust and demonstrate to the public and partners that integrity is at the heart of your data practices by being transparent about how data is collected, shared, transformed and used.

PUBLIC PARTICIPATION

Engage stakeholders, including members of the public who may be affected by data decisions, in the decision-making process. Public participation is generally viewed as a spectrum, ranging from less active modes of engagement, such as informing participants, to taking their input into account to guide decisions, to giving participants full participation in decision making.

Reasons for operationalizing this principle

1. Make informed decisions by accessing the collective intelligence of the public and incorporating feedback about their needs, values and concerns.
2. Engage audiences and earn trust in your work by concretely prioritizing their input in the decision-making process.
3. Support the common good by helping the public better understand your challenges and giving them an active role in decision-making processes.
4. Better understand the public's varied needs and expectations of your services by consulting and collaborating with them.

FRAMED EXPERIMENT

Balance between the use of experiment for iteration and for hypothesis testing, while adhering to other principles established in the data governance framework. In general, experiments should be conducted in accordance with the strategies defined in the governance framework and include clear documentation of the parameters of the experiment. However, if there is a need to deviate from the established strategies and principles in an experiment, it is the responsibility of the partners to justify this deviation and follow the procedures established by the City in this case. Such deviations must be exceptional and authorized when implemented in a framed manner: for a limited period of time, documented and subject to transparency criteria.

Reasons for operationalizing this principle

1. Solve problems previously identified with the audience.
2. Avoid the harmful effects of commercial lobbying.
3. Approach problem solving in a structured manner.
4. Build trust with the public and other partners by demonstrating that any experiment, whether or not it deviates from the principles, follows the City's established procedures.
5. Improve the effectiveness of your organization's services by testing new approaches and iterating on your existing approaches.
6. Manage risk through experimentation within the parameters established and documented by the City.

CYBERSECURITY

Measures put in place to protect or defend communication systems (computer hardware, software, etc.), and consequently the data they contain, against any use, modification, destruction, exploitation or dissemination, whether unauthorized or accidental. These measures are particularly important for the security of personal or sensitive data, or of any data that is valuable to cybercriminals, but their scope is broader. Cybersecurity measures cover a full lifecycle with risk prediction, mitigation and incident preparedness (response plan); mitigation of potential consequences (continuity plan); incident detection, response and then investigation; and communication with affected parties. This area is constantly evolving. It is therefore important to follow best practices on an ongoing basis.

Reasons for operationalizing this principle

1. Maximize service continuity for the public, minimize the risk of privacy breaches (if any) and thus maintain trust and credibility while reducing financial losses.
2. Consolidate the reliability of your data. Maintaining the security of the infrastructure that supports the data used ensures the integrity of the data used, whether internally or with external partners.
3. Be able to detect and respond effectively to an attack, thus maximizing the chances that the attack will fail.

INTEROPERABILITY AND DATA PORTABILITY

Data interoperability refers to the ability of systems and organizations to work together to use and share datasets semantically, technically, legally, and organizationally.

Data portability refers to the ability to transfer a dataset between different applications and systems and reuse it.

Reasons for operationalizing these principles

1. Benefit from the collective intelligence of colleagues and organizations by facilitating the current and future access, exchange and use of datasets.
2. Establish a shared view of accessible datasets using a common language (e.g. collection context, format) within and across organizations.
3. Acquire information and expand knowledge by combining datasets to support decision making, improve an organization's internal operations, and enhance or create new service offerings.

Reasons specific to data interoperability

4. Reduce the cost and effort associated with the current or future migration of a dataset between different systems, and thus enable some form of replicability.

Reasons specific to data portability

5. Contribute to avoiding technological lock-in of incompatible proprietary systems, and thus maintain healthy market competition.
6. Allow individuals to reuse datasets according to their needs (greater transparency on datasets, reuse in another service...).

DIGITAL SOBRIETY

An approach that takes into account the entire lifecycle of digital data. It proposes a reasoned collection, processing and use of data for specific, explicit and legitimate purposes.

Reasons for operationalizing this principle

1. Simplify data management by avoiding unnecessary data storage.
2. Limit the environmental impact of physical digital infrastructure.
3. Gain public and partner trust by explaining and validating the purposes of data collection and use.
4. Make strategic choices about the collection and use of data to ensure it meets objectives.
5. Be able to justify the purposes for which datasets are collected and used to guarantee that the privacy of stakeholders is respected.

INCLUSION

Process that ensures the meaningful participation of all people in the management and governance of their data (e.g. interpretation and consideration of data and results, uses of data, etc.), regardless of their age, sex, gender, disability, ethnicity, origin, religion, economic status or other statuses. Operationalizing this principle means considering removing barriers to the active participation of the individuals affected in all activities related to their data, especially for systematically underrepresented groups. In addition, where appropriate, it is recommended that the data collected be disaggregated to better detect any discriminatory phenomena specific to particular population groups (GBA+* approach) and to contribute to better representation in the data itself.

Reasons for operationalizing this principle

1. Reduce discrimination and numerical inequity due to underrepresentation in the data.
2. Leverage data by ensuring that the needs, values and rights of affected groups are respected and accurately reflected in all aspects of the management and governance of their data to combat discrimination and inequality.
3. Improve the quality and interpretation of your data by using a collaborative approach that promotes respect for differences between groups, while reducing oppression and bias.
4. Leverage data to better understand the impacts, challenges, opportunities, and lived experiences of various demographic groups in relation to your organization's services using an intersectional approach.

UNIVERSAL ACCESS

Ensures that data that can be used for the common good is locatable, understandable and usable by the public, as long as it does not infringe on sovereignty and individual or collective rights to privacy. Preserving and documenting data to ensure its accessibility allows for the equitable distribution of benefits, resources, and opportunities. Universal access relies on three conditions: 1) digital literacy (to equip people to use the data); 2) data availability; and 3) data management that clearly explains what the data represents, how it was produced, and how it can be used.

Reasons for operationalizing this principle

1. Maximize the impact of your work by ensuring that data is available and documented for easy interpretation and sharing.
2. Minimize social, economic, and political inequities by prioritizing accessibility and clarity of data for all.

ECOLOGICAL TRANSITION

Involves a trade-off between the positive and negative impacts of information and communication technologies (ICT). While these technologies may enable advances in environmental sustainability, they carry environmental costs. Consider the consumption of resources and the generation of waste resulting from the manufacturing, distribution, maintenance, and disposal of products and services related to these technologies as well as the impact of energy consumed by the operation of ICT applications. Partners can contribute to the ecological transition by using data and technology to advance environmental sustainability as well as practicing digital sobriety to minimize the negative impact of these technologies.

Reasons for operationalizing this principle

1. Support the common good by using the services your organization provides to promote the ecological transition and by employing sustainable practices within your organization.
2. Reduce your organization's environmental footprint while leveraging the benefits of digital sobriety.

COMMON GOOD

Using data for the common good means mobilizing it to build a more just society, overriding short-term considerations and the private interests of organizations or individuals. The application of this principle to data governance aims to improve our coexistence in a shared space and to strengthen the capabilities* of communities and individuals to lead the kind of life they have a right to desire. This application requires consideration of others (because people share the same space, their decisions impact others), collaborative governance* (any group should be able to meaningfully influence decisions that affect them), and reprioritization (fair decisions should benefit the most powerful groups only when it benefits groups that are systematically underrepresented).

Reasons for operationalizing this principle

1. Use data to innovate in ways that are relevant, legitimate, inclusive, fair, and sustainable, while rejecting data-mining practices that have led to significant power imbalances among stakeholders.
2. Contribute to a more equitable distribution of the value and benefits of data across the population. This is particularly relevant when the costs and risks resulting from experimentation, innovation, and use of data are publicly funded.
3. Improve the quality and interpretation of your data by using a collaborative approach that promotes respect for differences between groups, while reducing oppression and bias.
4. Recognize and support the diversity of needs by focusing on understanding the differential impact that projects, innovations, and interventions have on different groups, while limiting harm.
5. In the case of the smart city project "Montréal in Common", use data as commons* to improve access to fresh, local food and sustainable modes of transportation to improve the quality of life of Montréalers.

Logical links between principles

To understand the principles in the context of their interactions and nuances, it is important to have in mind the logical links between the different principles. These links are presented in a correspondence table that starts with each principle in the first column on the left (in red). We have classified them into three categories represented by colors:

- ➢ **TENSION**: The principles are in tension and limit each other in their respective scope of action.
- ➢ **SYNERGY:** The operationalization of the principle (left) supports a successful implementation of the other principle (top).
- ➢ **REQUIRED**: Operationalization of the principle (left) is required for successful implementation of the other principle (top)

	The right to privacy, personal and collective	Digital sovereignty	Consent
The right to privacy, personal and collective...		... includes the ability to control one's data, which is important for the sovereignty of individuals.	... justifies the importance of consent..
Digital sovereignty...	... of people supports the ability to remain anonymous.		... lays the foundation for consent.
Consent...	... formalizes the right to privacy.	... partially formalizes digital sovereignty.	
Transparency...	... must not infringe on privacy.	... allows individuals to know how their data is governed and used.	... is essential to build trust with the parties involved.
Public participation...			... promotes an open dialogue about what consent means to the public.
Framed experiment...	...must take steps to protect privacy.	... must take steps to protect digital sovereignty.	
Cybersecurity...	... avoids the exposure of personal and collective data.		
Data interoperability...		... must guarantee a place for other ways of describing the world.	
Data portability...	... must not infringe on privacy.	... provides access to and understanding of data, key elements to exercise digital sovereignty.	
Digital sobriety...	... limits the amount of personal and collective data collected.	... must allow for a diversity of ways to describe the world (e.g. multiple languages).	
Inclusion...	... needs disaggregated data to identify discrimination.	... guarantees an essential participation in sovereignty, even if sovereignty goes further.	...must ensure that the process of obtaining consent takes into account the many needs and perspectives.
Universal access...	... must not infringe on the right to privacy.	... seeks consensus with sovereign persons on what data should be universally accessible or not.	... supports meaningful consent (because people have an understanding of the data and the issues)
Ecological transition...			
Common good...		... recognizes the differences between groups and their right to influence decisions that affect them.	

	Transparency	Public participation	Framed experiment	Cybersecurity
The right to privacy, personal and collective...	... limits the disclosure and sharing of personal and collective data.		... must be protected during an experiment.	
Digital sovereignty...	... justifies the importance of transparent data governance and management.		... must be protected during an experiment.	
Consent...	... discloses the methods and reasons for data acquisition.		... is a key element in earning the trust of the parties involved.	
Transparency...		...about the intent, acquisition and use of data is required for meaningful public participation.	... regarding the experimentation is required (parameters of the experimentation, data collected, results, justification of failures of other principles).	... must not weaken cybersecurity.
Public participation...	... improves the way data governance is made public.			
Framed experimentation...		... can create opportunities for public consultation and input.		...must define responsibilities and accountability for cybersecurity.
Cybersecurity...	... requires hiding certain aspects of data and systems to better protect them.		... must be able to protect any data that concerns the public.	
Data interoperability...	... promotes a consistent description of the data (includes processes and purposes of use).	... provides a common basis for understanding the data.		... extends the scope of cybersecurity to multiple systems.
Data portability...	... gives individuals greater control over their data.			
Digital sobriety...				... must not weaken cybersecurity.
Inclusion...		... ensures that every voice, including those structurally underrepresented, is heard and incorporated into participatory processes.	... must not be weakened by an experiment.	
Universal access...		... supports meaningful public participation (because people have an understanding of the data and issues).		
Ecological transition...				
Common good...				

	Interoperability of data	Data portability	Digital sobriety	Inclusion
The right to privacy, personal and collective...		... shapes how personal or collective data should transfer from one service provider to another.	... limits the amount of personal and collective data collected.	... provides a framework for the use of disaggregated data, which is key to proving discrimination.
Digital sovereignty...	... shapes the context for data sharing and reuse.	... shapes how personal or collective data should transfer from one service provider to another.	... must be guaranteed before considerations of digital sobriety.	
Consent...		... is explicitly required before (re)use and sharing of data.		
Transparency...	... provides key information for potential collaboration around data.	... allows for a critical look at the data.		... allows groups to challenge data practices to ensure their needs, values and rights are respected.
Public participation...				
Framed experiment...				... should not have a negative impact on the fundamental rights of different groups.
Cybersecurity...	... ensures adequate protection of sensitive data at the time of their circulation.		... must be adequately guaranteed before considerations of digital sobriety.	
Data interoperability...		... is required for data reuse.	... increases the chances that relevant systems or data will be discovered and reused.	
Data portability...				... provides access to and understanding of data, reducing barriers to participation around data.
Digital sobriety...	... motivates the adoption of standards to limit collection and processing.			
Inclusion...				
Universal access...				... focuses on access to and understanding of data and reducing barriers to participation.
The ecological transition...			... motivates the importance of digital sobriety.	
The common good...			... involves specific, explicit and legitimate purposes for the use and collection of data.	

	Universal access	The ecological transition	The common good
The right to privacy, personal and collective life...	... limits the data that should be accessible.		... gives individuals and groups control over their personal and collective data.
Digital sovereignty...	... raises the question of which entity has the legitimacy to determine what data will be made publicly available.		
Consent...			... allows individuals or groups to influence the data acquisition phase to reflect their interests and needs.
Transparency...			... allows the sharing of information crucial to any collaborative approach.
Public participation...	... increases the means and capacities of the participating persons.		... is the only one who can define and negotiate the notion of common good.
Framed experiment...			... supports a deliberate and responsible approach that allows for transparency and accountability in decisions that impact others.
Cybersecurity...			... ensures that data is not diverted to private and short-term interests. It also supports the integrity of data and the continuity of digital services.
Data interoperability...	... provides common benchmarks for understanding the data.	... increases the chances that relevant systems or data will be discovered and reused.	... promotes collaboration between organizations. It can also support data sharing for the common good.
Data portability...	... provides access to and understanding of data, which is key to making access to certain data universal.		... allows the reuse of data to address long-term and collectively decided issues.
Digital sobriety...		... reduces the negative environmental impact of data and the technologies that support it.	
Inclusion...			... reduces systemic barriers and strengthens the ability of each person to lead the kind of life they have reason to desire.
Universal access...	▨		... promotes a more equitable distribution of the value and benefits of data.
Ecological transition...		▨	
Common good...		... prioritizes data uses that support a long-term vision, including sustainable living environments.	▨

Tactics

Tactics are the concrete actions you must take to comply with the Charter principles. This section presents a series of core tactics, organized by theme, that translate the Charter principles into guidelines. Be sure to distinguish between core tactics and operational tactics.

Core tactics

Core tactics are high-level actions that are implemented once at an organization or digital data partnership level and updated as needed. They may include writing policies, guidelines, and strategies, as well as choosing norms and standards.

Note that this data governance framework does not prescribe any existing norms or standards. The adoption of norms and standards is a strategic choice that must be aligned with the goals of an organization, partnership, or ecosystem. That said, Open North shares useful resources in this data governance framework that can serve as a starting point in operationalizing tactics, including the selection of relevant standards. New useful resources will be added to this document as we identify them during the capacity building program.

When combined, the core tactics can form a data strategy. You will have great flexibility in shaping these tactics to fit your needs and reality. Core tactics should be implemented in a way that is commensurate with the nature, importance and scale of your data activities.

Operational tactics

Operational tactics are field actions that are implemented by any stakeholder involved in a project (including data managers and project managers) when making decisions around their data use cases throughout the data lifecycle*.

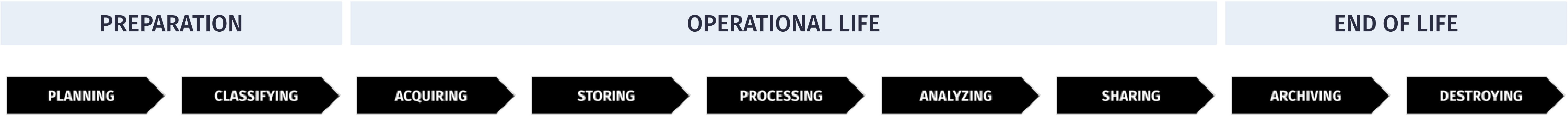


Figure 2: Montréal in Common’s digital data lifecycle

Operational tactics may apply to one or more stages of the data lifecycle shown in Figure 2. Note that each dataset may have a different lifecycle, so the datasets for which you are responsible will not systematically go through all the stages in Figure 2. This generic lifecycle should also be considered from the perspective of the copies of datasets you govern (whether for an organization or a partnership) and does not take into account copies of datasets governed by a third party.

Operational tactics are, for the most part, the applied and operational manifestation of core tactics applied to a use case*. As such, they provide opportunities to improve the core tactics in light of their application to real-life use cases. Complementary to the framework, Open North will provide you with a decision diagram entitled "**Data Use Case Decision Diagram**" that will guide you through the important steps and decisions of a data-driven use case. **In addition to the tactics documented in the framework, you will need to ensure that in planning your use cases, you have the resources to carry them out, clarify and assign roles and responsibilities for the governance and management of the data being used (both internally and at the partnership level), and identify training opportunities, where appropriate, to ensure that those assigned are empowered to fulfill their responsibilities.**

Core or operational tactics that are conditional

Finally, to accommodate the needs and realities of partners, both core and operational tactics can be **conditional**. As the name implies, conditional tactics apply to you only if you meet a particular condition, such as collecting or sharing personal or sensitive data. You will recognize a conditional core or operational tactic on the following pages by the icon (see box below) that accompanies it.

Special conditions that may make certain fundamental and operational tactics conditional:

🔒 Collection, use or sharing of personal or sensitive data

🗄[3] + 🔒 Use of an internal technological solution to collect personal or sensitive data

🖥[4] + 🔒 Use of an internal technology solution to share personal or sensitive data

🤝 Outsourcing of one or more stages of the data lifecycle associated with the theme in question (e.g. outsourcing the analysis of your data)

You will also find, for each theme, a **list of the results and benefits that** can be derived from the activation of the tactics that belong to the theme in question. We also believe that certain **favourable conditions** particularly support the consistent and sustainable implementation of the tactics. Together, we will be able to validate the relevance of these favourable conditions during the operationalization of the tactics, by sharing our learning.

[3] Royalty free icon source: Flaticon.com

[4] Royalty free icon source: Flaticon.com

Themes of the data governance framework

THEMES	DESCRIPTION
Define your use cases for the common good	This theme is intended to ensure that you are mobilizing your data to solve problems and create a more just society, and that you clearly define the success of the intended use case (whether exploratory or not).
Stakeholder engagement	This theme helps you build trust, mitigate damage, and improve data relevance throughout the lifecycle of your data use cases.
Monitoring of existing data	This theme helps you discover existing data that can support your use case.
Data acquisition	This theme applies if you need new data to support your use case.
Understanding and documenting the context of the data	These three themes support data that is understood, ready to be used, valued, and useful for its intended purpose. Specifically, understanding and documenting the context of data builds stakeholder confidence by transparently tracing decisions made around data throughout the data lifecycle of a use case. These 3 themes apply to both existing and new datasets. While the goal should be to prioritize the application of tactics belonging to these themes as much as possible in the planning stage, in practice, they also apply to other stages of a use case's data lifecycle.
Data quality	
Data interoperability	
Data classification	These two themes help you structure the consideration of key data aspects (such as legal requirements, risks, and stakeholder interests) by combining data classification very early in the lifecycle to better mitigate risk.
Risk management	
Data storage and access	This theme ensures that data is stored and accessed in a secure and responsible manner while reducing the environmental costs of data storage.
Data analysis	This theme supports the discovery of useful information as a means to achieve the goals set by each use case.
Data sharing and publishing	This theme aims to foster the transparent flow of information for the general public as well as collaborative opportunities to further mobilize data for the common good, while respecting collective and individual human rights in the digital age.
Data archiving	The following two themes help you manage the end of the data lifecycle, recognizing that underutilized data that still has value should be stored in a secure, intentional, and sustainable manner, while other data should be destroyed for ethical, legal, or operational reasons.
Data destruction	

When operational tactics are applied along the lifecycle of Montréal's shared digital data

LEGEND

✓ means operational tactics apply for this digital data lifecycle step

	PREPARATION		OPERATIONAL LIFE					END OF LIFE	
	PLANNING	CLASSIFYING	ACQUIRING	STORING	PROCESSING	ANALYZING	SHARING	ARCHIVING	DESTROYING
Define your use cases for the common good	✓								
Stakeholder engagement	✓	✓	✓	✓	✓	✓	✓	✓	✓
Monitoring of existing data	✓								
Data acquisition	✓		✓						
Understanding and documenting the context of the data	✓	✓	✓	✓	✓	✓	✓	✓	✓
Data quality	✓		✓		✓	✓	✓		
Data interoperability	✓		✓	✓	✓		✓		
Data classification		✓							
Risk management	✓	✓	✓	✓	✓	✓	✓	✓	✓
Data storage and access	✓	✓		✓			✓		
Data analysis					✓	✓			
Data sharing and publishing					✓		✓		
Data archiving								✓	
Data destruction									✓

1. Define your use cases for the common good

This theme is intended to ensure that you are mobilizing your data to solve problems and create a more just society, and that you clearly define the success of the intended use case (whether exploratory or not).

Key principles

- Common good
- Public participation
- Inclusion
- Framed experiment
- Ecological transition
- Digital sovereignty

Favourable conditions

- Strategic oversight and vision
- Communication skills

Results

- Be transparent about the challenges you face and aware of the risks to groups or individuals.
- Mobilize data as a means of addressing real needs and identifying more effective and just solutions.

Core tactics	Operational tactics
Tactic 1.1 Involving all relevant stakeholders, define and document the overall values your organization or partnership seeks to generate through the use of its data and how the use of data can contribute to the common good (see definition of principles).	**Tactic 1.1.1** Before developing the solution, take time to explore the problem(s) the use case seeks to solve, including stakeholder analysis, historical, political and cultural context. Study previous efforts to solve it, including non-digital solutions. Document what you have learned in simple, clear words. **Tactic 1.1.2** Identify the desired outcome(s) of the use case, the indicators of success, and the conditions for success. *Note: This is an essential basis for tracking and collecting learnings and evaluating your use case.* **Tactic 1.1.3** Demonstrate that the desired outcome(s) and process of the use case support the principle of common good, as defined. **Tactic 1.1.4** Consider whether a data-driven intervention would be useful in addressing the problem. If so, think about the type of data needed to achieve the goals of the use case and the potential limitations of that data.
Tactic 1.2 Integrate the overall values and associated goals related to data use into robust organizational monitoring and evaluation processes.	**Tactic 1.2.1** When the use case ends (either completed or not), evaluate the project and its results against what was planned and share lessons learned.

Did you know?

Comparing data with cars helps us understand some key points: driving is not just about avoiding tickets, and governing data goes beyond legal compliance in order to make your data your ally in achieving your goals. The strategic vision in data governance is as important as a GPS indicating the direction. The person responsible for data governance is driving, but must take into account other stakeholders (like a driver pays attention to pedestrians, bikes, buses ...). It is also interesting to raise the challenges of a car-based society, as well as data-based, and negotiate what the common good means.

Purpose and processes are at least as important as data. For example, disaggregated data is critical to the GBA+ cross-sector approach but can also reinforce stigmatization of communities if not accompanied by a "process whose goal is to reduce systemic racism and oppression and establish equity." - Executive Summary of this report.

Useful resources

The City of Montréal's GBA+ 101 Guide (in French), to understand and incorporate a GBA+ approach into your practices. (NB: Incorporating a GBA+ approach into projects will be increasingly required by the City). To go further: GBA+ toolkit for public participation (in French); the OCPM report on racism and systemic discrimination: All the opinions of the Conseil des Montréalaises, which has long included GBA+ in its work.

2. Stakeholder engagement

This theme helps you build trust, mitigate damage, and improve data relevance throughout the lifecycle of your data use cases.

Key principles

- Transparency
- Public participation
- Inclusion
- Digital sovereignty

Favourable conditions

- Skills and training
- Strategic oversight and vision
- Clear and shared data culture
- Communication skills

Results

- Build public trust in your work by being transparent about your data governance practices and valuing public input into the decision-making process.
- Make informed decisions through a better understanding of the diverse needs and expectations of the public.
- Protect basic digital rights.
- Improve the quality of your data by relying on collective intelligence, as well as on a diversity of viewpoints, opinions and expertise.

Core tactics	Operational tactics
Tactic 2.1 Publish (e.g. on a website) and distribute by any means that will likely reach relevant stakeholders all of your relevant data governance policies and practices using a readable and easy-to-understand format. Clearly explain how an individual can give you feedback or ask questions about your data governance and how you will handle it. Make sure this information remains current. *Note: This includes publishing contact information for the person responsible for privacy practices (if applicable) as well as information about how an individual or group can access their personal data. More broadly, this legal requirement is an opportunity to support stakeholder engagement on data governance and use.*	**Tactic 2.1.1** Establish an inclusive strategy on how to engage and consult with all stakeholders affected or likely to be affected by data-related decisions throughout the use case, as appropriate (with an emphasis on engagement and consultation prior to the use case in question).
Tactic 2.2 🔒 Develop a process for handling complaints and investigations related to personal data privacy issues and communicate it publicly. *Note: Act 25 (The Modernization of Personal Information Protection Legislation) requires organizations to have a complaint process in place and to respond to an individual's request for access or correction within 30 days (source)*	**Tactic 2.2.1** 🔒 Deal with all complaints in a timely manner. *Note: Steps may include recording and reviewing the complaint, making any necessary changes or corrections, and notifying the person who filed the complaint of its resolution.*

Did you know?

Your team and partners will also benefit from clear documentation of your data governance. This OBVIA guide (in French) presents 7 issues related to the use of technologies on marginalized populations: exacerbation of pre-existing inequalities; stigmatization with the collection of large quantities of potentially sensitive data; issues for allophones; exclusion of populations; indirect exclusion of populations; issues of trust and social acceptability; issues of data quality and integrity. Hence the importance of "consulting the populations involved and the organizations that represent them in order to determine needs and priorities" as well as "the participation of the stakeholders and groups affected in the data analysis and interpretation process".

Useful resources

Resource to get started with the Web Content Accessibility Guidelines (WCAG) (NB: the publication of the WCAG 2.2 standards is scheduled for June 2022). In smart city projects, residents are likely to be a stakeholder. This guide (in French) "for all project leaders who want to implement citizen participation, especially for the most disadvantaged" could help you start your reflection, as well as the Passerelle Public Participation community. It is also worth mentioning this report dedicated to participatory frameworks in the context of data use.

3. Monitoring of existing data

This theme helps you discover existing data that can support your use case.

Key principles

- Transparency

Favourable conditions

- Strategic oversight and vision
- Tools and techniques

Results

- Have a complete and easily accessible view of the data that is of strategic value to your organization or partnership.

<table>
<tr><th>Core tactics</th><th>Operational tactics</th></tr>
<tr><td>**Tactic 3.1**
Create and maintain a catalog of all **strategically valuable** data assets held by your organization or partnership, including open data.
Notes:
- *Updates to the data catalog should be integrated into the workflow;*
- *The data catalog may also contain links to external data sources that may be of future interest but are not yet in your possession.*</td><td>**Tactic 3.1.1**
Assess whether existing and available datasets can suffice for the use case.</td></tr>
<tr><th colspan="2">Did you know?</th></tr>
<tr><td colspan="2">In order to make the data catalog useful and utilized, remember to incorporate regular updates into your work habits. You can look for both internal (also called closed) data and open, shared data (report p.46), even if you do not have access to it yet.
The *Modernization of Personal Information Protection Legislation Act* (Act 25) updates some 20 provincial statutes, primarily the *Act respecting the protection of personal information in the private sector* and the *Act respecting access to documents held by public bodies and the protection of personal information*.
Digital sobriety and respect for the right to privacy call for the minimization of data collection. This is facilitated by monitoring existing data. However, the trend is rather to the proliferation of digital activities, which induces an increase of 9% in energy consumption. This is due at 55% to its use and at 45% to its production. (source). On the data protection side (necessary to respect privacy), keeping data is dangerous because it is difficult to secure and failure to secure data leads to significant damage. (source)</td></tr>
<tr><th colspan="2">Useful resources</th></tr>
<tr><td colspan="2">N/A</td></tr>
</table>

4. Data acquisition

This theme applies if you need new data to support your use case.

Key principles

- Digital sobriety
- Ecological transition
- Right to privacy
- Inclusion
- Consent

Favourable conditions

- Strategic oversight and vision
- Skills and training
- Legal expertise
- Communication skills

Results

- Use valuable, fit-for-purpose-data while minimizing environmental risks and costs
- Ensure legal compliance in the collection of sensitive or personal data
- Protect fundamental rights in the digital age, such as consent and privacy rights
- Hold third-party providers responsible for collecting data on your behalf

Core tactics	Operational tactics
Tactic 4.1 Define a data acquisition strategy* that balances the relevance* of data (including the ability to capture context) with the benefits of data minimization* processes.	**Tactic 4.1.1** Plan to acquire only the most significant and necessary data to achieve the objectives established by the use case. **Tactic 4.1.2** Assess whether the acquisition of sensitive or personal data (including disaggregated data*) is absolutely necessary to effectively meet the objectives of the use case. *Note: A GBA+* approach often requires obtaining personal data disaggregated by a particular subgroup (e.g. an immigrant community). The very existence of this data is a risk to that community, which is in the best position to decide whether the risk is worth taking.* **Tactic 4.1.3** 🔒 Determine a strategy to ensure that the new data entered is representative of the groups or individuals involved in the use case.
Tactic 4.2 🔒 Write and publish a data privacy policy, accessible to all relevant groups or individuals, that documents rules in simple terms to protect personal or sensitive information during the **data acquisition phase and beyond**.	**Tactic 4.2.1** 🔒 Apply tactics **8.2.1** and **9.1.2** before entering personal or sensitive data. **Tactic 4.2.2** 🔒 Assess whether your data capture methods are effective in obtaining clear, free and informed consent* for specified and legitimate purposes from the individuals or groups involved, and if not, reassess your data acquisition strategy. **Tactic 4.2.3** 🤝 Require the third party that will be capturing data on your behalf to sign a confidentiality agreement (if applicable) and a service level agreement with defined terms of use that are aligned with this governance framework and its principles.

Did you know?

The Limits to Digital Consent report shares 6 findings about the limits of consent, including that the current model is outdated, that it combines high potential for harm with indifference from decision makers, that everyone is at risk, that local data storage is not safer for individuals, and that platform designers should see themselves as potential negative actors. "Employment status and income, for example, would predict intensity of technology use, but also traces of online activity." This leads to underrepresentation. (p.11 of the report Les angles morts des réponses technologiques à la pandémie de COVID-19). According to the *Modernization of Personal Information Protection Legislation Act*, consent must meet the following 5 criteria: Clear, free, informed, given for specific purposes, and of some duration necessary to achieve the purposes for which it was requested. (source)

Useful resources

Open North’s Learning Management Platform offers a (free) course named "Setting up a Privacy Policy". Although it is more suited to municipal organizations, it can help you quickly understand key elements of such a policy in the context of a smart city. Among other things, this GDPR developer's guide provides guidance on minimizing the collection of personal information.

5. Understanding and documenting the context of the data

Along with **data quality** and **data interoperability**, these themes support data that is understood, ready to be used, valued, and useful for its intended purpose. Specifically, understanding and documenting the context of data builds stakeholder confidence by transparently tracing decisions made around data throughout the data lifecycle of a use case. These 3 themes apply to both existing and new datasets. While the goal should be to prioritize the application of tactics belonging to these themes as much as possible in the planning stage, in practice, they also apply to other stages of a use case's data lifecycle.

Key principles

- Transparency
- Data interoperability
- Data portability
- Digital sovereignty
- Universal access

Favourable conditions

- Tools and techniques
- Technical skills

Results

- Ensure a consistent understanding of the data so that it is used appropriately
- Identify and correct any misunderstandings of the data and its meaning

Core tactics	Operational tactics
Tactic 5.1 Adopt standardized practices* for referencing and accessing metadata* associated with the data under your responsibility. *Note: Some standard elements found in metadata include: origin, location, definitions of data variables, who was involved in its lifecycle, what choices were made in processing and analysis, how the dataset is cited, etc.).*	**Tactic 5.1.1** Ensure that metadata is documented according to defined standards and accessible in a machine-readable format. **Tactic 5.1.2** Document the relevant decisions, made at each stage of the lifecycle, that impact the data.

Did you know?

The purpose of a data glossary (also called a *business glossary*) is to improve the understanding and use of data across your organization. It should therefore be unique. Not to be confused with data dictionaries, which are more technical and dependent on information systems. (source)

Useful resources

N/A

6. Data quality

See the summary for **understanding and documenting the context of the data**.

Key principles

- Data interoperability
- Transparency
- Inclusion
- Universal access

Favourable conditions

- Tools and techniques
- Skills and training
- Strategic oversight and vision
- Communication skills

Results

- Ensure that the data is useful for the purposes identified
- Increase levels of confidence in the data for all stakeholders

Core tactics	Operational tactics
Tactic 6.1 Define and document a set of appropriate data quality standards applicable to various datasets used within your organization or partnership. *Note: There are many data quality standards. These are good starting points. Statistics Canada, for example, has defined 6 dimensions of data quality: relevance, accuracy, timeliness, coherence, interpretability and consistency.*	**Tactic 6.1.1** Determine and document the most appropriate data quality standards for the use case in question. **Tactic 6.1.2** Evaluate and verify that the data meets quality requirements and share the results of the evaluation with relevant stakeholders.

Did you know?

According to the Harvard Business Review article "Only 3% of Companies' Data Meets Basic Quality Standards" published in 2017, on average, 47% of newly created data has at least one critical error (e.g. an error that impacts work).

Useful resources

Statistics Canada defines 6 main dimensions of data quality and presents them in this video: relevance, accuracy, timeliness, interpretability, coherence and accessibility. See also this toolkit on data quality.

7. Data interoperability

See the summary for **understanding and documenting the context of the data**.

Key principles

- Data interoperability
- Data portability
- Universal access

Favourable conditions

- Tools and techniques
- Skills and training
- Strategic oversight and vision
- Communication skills

Results

- Ensure your data is ready to use
- Support data integration, interoperability, and portability
- Combine and cross-reference data
- Ensure a consistent understanding of the data so that it is used appropriately

Core tactics	Operational tactics
Tactic 7.1 Adopt consistent naming conventions for variables in the datasets you are responsible for. *Note: Naming conventions should include any reference codes for the common indicators identified for the mobility and food systems components of MiC.*	**Tactic 7.1.1** Name your data variables with the unique identifiers and standard codes identified by your organization or partnership's data strategy.
Tactic 7.2 Describe how structured data should be organized in an ordered format.	**Tactic 7.2.1** Follow the necessary steps to transform, correct and format your data according to the defined standards. *Note: For tactics **7.1.1 and 7.2.1**: If existing datasets are not properly standardized, notify the person(s) responsible to the dataset of the required changes.*

Did you know?

The *Modernization of Privacy Legislation Act* will require, as of September 2024, that upon request, organizations be required to disclose computerized personal information collected from an individual in a structured and commonly used technological format. (source)

Useful resources

N/A

8. Data classification

Along with **risk management**, these two themes help you structure the consideration of key data aspects (such as legal requirements, risks, and stakeholder interests) by combining data classification very early in the lifecycle to better mitigate risk.

Key principles

- Right to privacy
- Digital sovereignty

Favourable conditions

- Skills and training
- Clear and shared data culture
- Legal expertise

Results

- Improve your risk management and data security processes
- Know what type of data your organization or partnership holds, what laws apply to that data, and who should have access to that data
- Ensure legal compliance in the way you administer data

Core tactics	Operational tactics
Tactic 8.1 Develop a data classification system appropriate to the types of data used. *Note: There are several types of classification to better understand data, such as subject or content, origin, format, standards or norms applied or applicable, function, domain, degree of openness and degree of sensitivity. The degree of openness and the degree of sensitivity are particularly important in assessing the risks associated with a dataset. Other important classifications related to data sovereignty include Indigenous data and general interest data.*	**Tactic 8.1.1** In accordance with your classification system, categorize the data you plan to use according to the level of sensitivity, openness, and other categories of interest. *Note: This classification process must take into consideration issues of collective data sovereignty, such as data sovereignty for Indigenous communities or municipalities.*
Tactic 8.2 Document and track changes and amendments to data management legal requirements throughout the data lifecycle. *Note: Special attention must be paid to personal or sensitive data during the collection, analysis and sharing phases.*	**Tactic 8.2.1** Make sure you meet all compliance requirements (with regard to the law, to the tactics of this framework, and to any other conditions of use and access) for the data, if applicable.

Did you know?

According to the *Modernization of Privacy Act*, personal information is sensitive when, by its nature or the context of its use or disclosure, it gives rise to a high reasonable expectation of privacy (source).

The *Québec Charter of Human Rights and Freedoms* guarantees the right to privacy. The *Modernization of Personal Information Protection Legislation Act* (*Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*) aims to protect personal information, which may be public or private.

Useful resources

De-identified data and personal data can be treated differently. However, this report recommends that equal attention be paid to disaggregated data, whether personal or de-identified (pages 7-8). Technological advances will make it increasingly easy to re-identify data.

The Commission d'accès à l'information du Québec offers an evolving online space (in French) to learn more about the modernization of personal information protection laws in Québec. NB Keep in mind that depending on your context, you may be required to respect other legal, regulatory or contractual obligations.

This report explains some possible classifications of data (pages 42-47): their domain (personal, private, public), degree of openness (closed, shared, open) and origin (freely provided, observed, derived, inferred, purchased).

9. Risk management

See the summary for **data classification**.

Key principles

- Cybersecurity
- Right to privacy

Favourable conditions

- Skills and training
- Clear and shared data culture
- Legal expertise

Results

- Understand the risks associated with data use and mitigate potential harm

Core tactics	Operational tactics
Tactic 9.1 Develop guidelines on 1) how to assess risks that could harm data and information systems and 2) how to proactively mitigate those risks	**Tactic 9.1.1** Identify the risks to the data use case. *Note: Be sure to ask the following questions: could the use case generate new harms to individuals or society? Could the use case unfairly benefit or harm certain populations over others? Other common risks include data privacy incidents, security breaches, use of erroneous or inaccurate data, and aggregation or correlation of incompatible datasets.* **Tactic 9.1.2** 🔒 Conduct a privacy impact assessment before making decisions about collecting or sharing personal or sensitive data. **Tactic 9.1.3** If you can, implement appropriate strategies throughout the data lifecycle to mitigate the identified risks, and if not, re-evaluate your use case strategy. *Note: This tactic invites mitigation of risks identified in other tactics (4.1.2, 8.2.1, 9.1.1, 9.1.2, 11.1.3, 12.1.2, 12.1.3, 12.1.4, 14.1 and to some extent 4.2.3, 6.1.2, 10.4.3, 11.1.4). Note that other tactics already involve the implementation of mitigation (10.1.1, 10.4.1, 10.4.2).*
Tactic 9.2 🔒 Create and maintain a record of privacy and security incidents.	**N/A**

Did you know?

A privacy impact assessment evaluates the impact that a project, initiative or policy may have on the privacy of individuals. This can be done at the planning stage or when considering a major change. This allows for effective communication of privacy risks to stakeholders, including decision-makers, and the formulation of recommendations. The assessment is aimed at making informed decisions to respect privacy rights.

Useful resources

The *Privacy Modernization Act* will require privacy impact assessments in some cases, and the government is developing resources to assist in the implementation of this measure (in French). While these requirements only cover individual privacy, the reality of the age of big data and the legitimate demands of certain communities to be taken into account also require an analysis of the risks to group privacy.

Appendix C of this document (set in the context of New Zealand) provides a grid for analyzing privacy risks and possible measures to mitigate them. (pages 19-34)

10. Data storage and access

This theme ensures that data is stored and accessed in a secure and responsible manner while reducing the environmental costs of data storage.

Key principles

- Universal access
- Digital sovereignty
- Inclusion
- Right to privacy
- Cybersecurity
- Ecological transition
- Digital sobriety

Favourable conditions

- Technical skills
- Tools and techniques
- Clear and shared data culture

Results

- Ensure that data is available for future access (when permission is granted) without requiring all individuals to create their own copies
- Protect data from unauthorized access and mitigate risks such as data leakage, data loss or system failure
- Minimize the energy consumption of your data storage by keeping your database clean

Core tactics	Operational tactics
Tactic 10.1 Establish a strategy that aligns data storage needs with functional and controlled access mechanism provisions. *Note: This policy should include a protocol for configuring access to datasets, taking into account the user's role and the type of data.*	**Tactic 10.1.1** Define clear terms of access to data for all stakeholders and third parties. **Tactic 10.1.2** Assign permissions or privileges by role and configure access to minimize the need for unnecessary copies of the same data set. *Note: Although not a systematic rule, you can follow the principle of least privilege, i.e. a user should be given the minimum level of access necessary to perform a task or job.*
Tactic 10.2 🖥 + 🔒 Integrate an access control list as a feature to your technology solution.	**N/A**
Tactic 10.3 Establish a comprehensive data retention policy* tailored to your needs. *Note: This policy should establish in plain language a records retention schedule that identifies minimum and maximum retention and disposal periods for legal and operational purposes. It therefore covers archiving and destruction of data.*	**Tactic 10.3.1** Follow storage limitation practices, i.e. you should not retain data longer than necessary for one or more specified, legitimate and explicit purposes. **Tactic 10.3.2** Integrate your data into the records retention schedule, taking into account classification, risk management, and data collection steps. *Note: This tactic involves integrating your data into your records retention schedule. To do this, it is important to consider the classification, risk management and data collection steps.*
Tactic 10.4 🤝 Ensure that the third parties supporting your storage, archiving and destruction needs meet the requirements outlined in the service level agreements.	**Tactic 10.4.1** Have data backups to ensure that you can recover it in case of a computer system failure. **Tactic 10.4.2** Take reasonable steps to minimize the risk of harm from a data breach and to prevent similar incidents from occurring in the future. **Tactic 10.4.3** Record data breaches in the risk log and inform all relevant stakeholders of an incident.
Tactic 10.5	**N/A**

Develop an information system response and business continuity plan in the event of a potential data or computer system breach. *Note: The information system continuity plan includes plans for data backup (redundancy) and recovery from an incident.*	

Did you know?

The data retention periods defined in the policy of the same name can in practice be shortened with the exercise of the right to be forgotten by data subjects. (source, GDPR context).

While the root cause of a specific data breach may be varied (e.g. opportunistic theft, targeted hacking, employee negligence), any organization can mitigate the underlying causes (e.g. staff capabilities and attention, adequacy of safeguards, access rules, quantity and sensitivity of data held, governance and monitoring). (source).

Establishing strong password guidelines, regular updates, etc. are all reasonable measures to minimize the risk of harm from a data breach. Data backups are useful in the event of "loss, theft, failure, hacking or destruction of your digital devices." (source)

Note that the same data protection laws apply to the original data and its copy(ies). The number of perpetrators of cyber threats is on the rise and they are becoming more sophisticated. (source)

Useful resources

This report (in French) can be used as a starting point for access management. Keep in mind that it is set in the context of public bodies, prior to the reforms of the *Modernization of Privacy Legislation Act* and C-11.

This article summarizes the principles and best practices for retaining and destroying personal information. It may inspire practices for other types of data.

The Canadian Centre for Cyber Security offers resources for "small businesses" to strengthen their cyber security at low cost and with little strain. The first resource is the development of a response plan.

Ensuring that only authorized individuals can access data is part of the internationally recognized Five Safes model: Safe Data, Safe Projects, Safe People, Safe Settings, Safe Outputs. (page 6 of the document).

This Wikipedia article presents several methods of data deduplication (technical point of view).

This blog post (in French) shares best practices for managing data backup. Note that this is in the French context, not the Québec context.

Checklist (in French) prepared by the Commission d'accès à l'information du Québec to prevent security incidents. They focus on personal data here, but this could inform a more global approach.

In addition to developing a contingency plan, it is also possible to develop a business continuity plan. The benefits of this approach are listed in this short presentation, accompanied by a more complete guide (In French, the framework is broader than just cybersecurity).

11. Data analysis

This theme supports the discovery of useful information as a means to achieve the goals set by each use case.

Key principles

- Transparency
- Inclusion
- Public participation

Favourable conditions

- Technical skills
- Strategic oversight and vision
- Questioning and learning

Results

- Ensure that individuals can scrutinize the results of algorithms or calculations and understand the logic and reasoning behind decisions about their data
- Improve your data analysis by drawing on the perspectives and insights of all stakeholders
- Hold third-party providers who analyze data for you responsible
- Enable reproducibility and audits of analytical processes

Core tactics	Operational tactics
Tactic 11.1 Document the different types of data analysis used within your organization or partnership, both in-house and with a third party. Specify the requirements for conducting the analyses (e.g. documentation of processing and analysis performed, reproducibility, audits, stakeholder engagement) and the limitations of each type of analysis. *Note: Because some decisions based on data analyses will have real-life consequences, it is crucial to be able to explain the logic and reasoning behind these decisions. If this is not possible, you may want to look for other analytical methods that allow for an appropriate degree of explicability.*	**Tactic 11.1.1** Determine the appropriate analysis techniques for your use case. **Tactic 11.1.2** Document relevant aspects of the analysis process to enable reproducibility and audits. *Note: Important aspects to be documented may include, but are not limited to, descriptions of the data considered in the analysis, the techniques used to analyze its content or quantitative component (or statistical techniques), the algorithms and analytical assumptions used, and the results.* **Tactic 11.1.3** Before publication and as a rule, get a feedback loop on your analysis process and results by presenting the analyses and their findings in a clear and actionable way to all relevant stakeholders. **Tactic 11.1.4** 🤝 Require the third party that will be analyzing the data on your behalf to sign a confidentiality agreement (if applicable) and a service level agreement with defined terms of service, including requiring full transparency about the analysis process. Take steps to ensure that you can verify the analysis and the appropriateness of the findings before relying on them. *Note:* To verify the validity of the findings, you can ensure you have the *capabilities in-house, partner with a trusted organization to verify the work, or even create a list of verified trusted providers with reliable analysis capabilities.*

Did you know?

The partnership approach to research has the following characteristics:

- Community-centred;
- Based on equitable sharing of decision-making power throughout the project with the community;
- Proposes a process and results that are useful to the community.

It allows us to produce new knowledge in a more robust way and to equip the community to solve pressing social issues. (source).

Useful resources

Regarding quantitative analyses: 7 steps toward more transparency in statistical practice: (1) Visualizing data; (2) quantifying inferential uncertainty; (3) Assessing data preprocessing choices; (4) Reporting multiple models; (5) Involving multiple analysts; (6) Interpreting results modestly; and (7) Sharing data and code. (The findings are general enough to be useful outside the social and behavioral sciences).

12. Data sharing and publication

This theme aims to foster the transparent flow of information for the general public as well as collaborative opportunities to further mobilize data for the common good, while respecting collective and individual human rights in the digital age.

Key principles

- Transparency
- Inclusion
- Right to privacy
- Cybersecurity
- Transparency
- Digital sovereignty
- Data interoperability
- Data portability
- Public participation

Favourable conditions

- Technical skills
- Tools and techniques
- Clear and shared data culture

Results

- Ensure that individuals can scrutinize the results of algorithms or calculations and understand the logic and reasoning behind decisions about their data
- Improve your data analysis by drawing on the perspectives and insights of all stakeholders
- Hold third-party providers who analyze data for you responsible
- Enable reproducibility and audits of analytical processes

Core tactics	Operational tactics
🔒 Refer to **Tactic 4.2** (data privacy policy) which also documents the rules to follow to protect personal and sensitive data during the sharing and publishing stage.	**Tactic 12.1.1** Apply tactic **8.2.1** before sharing your data. *Note: The decision to share or not share a dataset must also consider whether it will be used for purposes consistent with those for which the data was originally collected. It must also be aligned with the principle of mobilizing data for the common good as defined in this document.* **Tactic 12.1.2** 🔒 Apply tactic **9.1.2** before sharing your personal and sensitive data. Then make sure you do not share data that could generate individual or public harm (beyond any privacy protections). **Tactic 12.1.3** 🔒 Before publishing or sharing data, determine the appropriate techniques to protect the data and minimize the risk of re-identification. *Note: Techniques may include redaction of commercially sensitive numbers or names, pseudonymization, anonymization, or aggregation of personal information, and application of the "programmed privacy" principle for technology solutions.* **Tactic 12.1.4** 🔒 If you disclose personal information, you must first enter into a data sharing agreement with the person, organization or partnership to whom it is disclosed, clearly stating the terms of use and access to the data (Act 25). *Note: Beyond ensuring protection of personal and sensitive data, data sharing agreements can be used to ensure that data containing information about the environment or the built environment, for example, is systematically mobilized for the common good.* **Tactic 12.1.5** Indigenous or general interest data must be returned, using the appropriate formats, to the appropriate Indigenous community or the City of Montréal respectively. Individuals must also be able to request and obtain access to their personal information.

Did you know?

There are two families of techniques for anonymizing data: randomization and generalization. How to verify the effectiveness of anonymization? By verifying that it is not possible to isolate an individual in the dataset (individualization); to link together distinct datasets concerning the same individual (correlation); or to deduce, in a quasi-certain way, new information about an individual (inference). (source). The foundations of a successful digital data partnership are creating a climate of trust conducive to collaboration and seeking positive social impact in the public interest. (source)

Useful resources

This report provides important recommendations for establishing digital partnerships. It is designed for the Québec context, and does not go into the details of drafting a data sharing contract.

13. Data archiving

Along with **data destruction**, these two themes help you manage the end of the data lifecycle, recognizing that underutilized data that still has value should be stored in a secure, intentional, and sustainable manner, while other data should be destroyed for ethical, legal, or operational reasons

Key principles

- Ecological transition
- Cybersecurity

Favourable conditions

- Strategic oversight and vision
- Legal expertise
- Tools and techniques

Results

- Keep little used but potentially valuable data while staying within a reasonable storage budget

Core tactics	Operational tactics
Tactic 13.1 As a complement to Tactic **10.3**, design your archiving strategy around your data classification efforts (Tactic **8.1**) by determining the useful life of different data types.	**Tactic 13.1.1** Following your data retention guidelines, monitor the activity on your dataset and its relevance to future use cases to determine if it should be archived.
Tactic 13.2 In addition to tactics **10.1** and **10.3**, ensure that data can be retrieved from the archive as needed and determine who can access the archived data.	**N/A**

Did you know?

"The question is less what can be preserved so much as what should not be lost." (source) All stakeholders are to be considered. What might seem unimportant to you could be of major interest to a local historical society or an Indigenous community.

"Selection, appraisal and disposal are significant components in any digital management activity. In the context of an expanding digital universe, a determined effort to identify, process and retain digital material of enduring value means on one hand that the right material is available to the right people at the right time in the right format; and on the other hand material is identified that can be actively removed or benignly neglected" (source)

Useful resources

Digital Preservation Coalition Handbook (in French), and the Handbook's User Guide (in English).

14. Data destruction

See the summary for **data archiving**.

Key principles

- Ecological transition
- Cybersecurity
- Right to privacy
- Consent

Favourable conditions

- Legal expertise
- Tools and techniques

Results

- Minimize energy consumption linked to your data storage by keeping your database clean
- Comply with the retention requirements, if any, associated with your data
- Protect the right to privacy

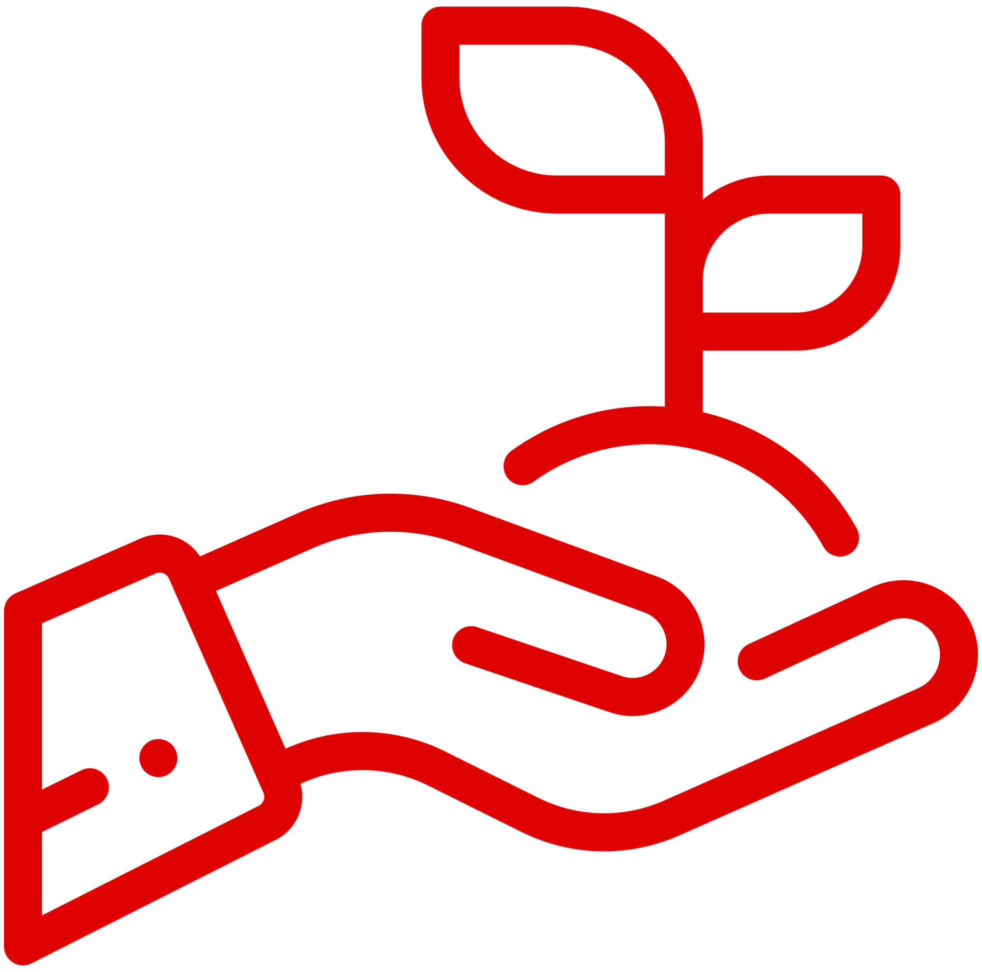
Core tactics	Operational tactics
Tactic 14.1 As a supplement to Tactic **10.3**, develop and document a destruction process describing the steps necessary to destroy data.	**Tactic 14.1.1** If applicable, set a reminder for data destruction based on your records retention schedule. **Tactic 14.1.2** Ensure the irretrievable destruction of all copies of a dataset that is to be destroyed.

Did you know?

It is not enough to delete data - especially personal data - and empty the bin to ensure that it cannot be reconstructed. To do this, other methods must be used, such as the total destruction of the medium (digital or analog), the deletion of the information with methods that can withstand basic recovery procedures (e.g. "overwriting" the original content of the media) and the demagnetization of the magnetic medium. (source)

Useful resources

N/A



Together, we can cultivate a more responsible, effective and collaborative data governance.

This is the first iteration of the Montréal in Common Data Governance Framework. In the spirit of continuous evaluation and improvement, this framework will evolve. You can help shape it! Please send your questions, comments, feedback or ideas to the following email address: mec@opennorth.ca.

What's next on your data governance journey?

Assess where you are in implementing tactics with the data governance self-assessment tool.