Commission d'accès à l'information du Québec

Conducting a privacy impact assessment

Companion guide

September 22, 2023

This document is an unofficial translation provided as a courtesy by Dentons Canada LLP's Privacy and Cybersecurity Group. This document is intended for informational purposes only.

Version 3.0

September 22, 2023

This guide was developed by the Commission d'accès à l'information in 2021. This new version takes into account the *Act to modernize legislative provisions respecting the protection of personal information* (Act 25).

Administrative versions of the *Act respecting access to documents held by public bodies and the protection of personal information* and the *Act respecting the protection of personal information in the private sector,* incorporating the most recent amendments, are available on the Commission's website: https://www.cai.gouv.qc.ca/. The text of this guide **does not take** into **account** possible changes brought about by bills under consideration, or not yet in force, at the date of publication of this guide.

This guide is a support tool. The concepts it contains are informative and are intended to aid understanding. In the event of contradiction between the information presented and the actual terms of the laws, the latter will prevail.

Public and private organizations are responsible for ensuring that they comply with the legal framework in force for the protection of personal information.

The gender neutral terms "they", "them", and "their" are used to refer to any person.

 If you have any comments about this guide, please contact us at veille@cai.gouv.qc.ca. Please note that we will not necessarily respond to these comments, but will take them into account when considering future updates to the guide.

For official documents, please visit the Commission d'accès à l'information's website at the following address: https://www.cai.gouv.qc.ca/.

Table of contents

About this guide

What is its purpose?

This guide is designed to **help** you **carry out a Privacy Impact Assessment (PIA),** whether you're doing it because of a legal obligation or as a matter of good practice.

Examples of projects:[1]

- Development of a new information system or personalization technique for a product or service;
- Purchase of an artificial intelligence system or surveillance cameras;
- Fingerprinting, geolocation, facial recognition, connected objects and sensors for smart cities;
- Communication of personal information to a researcher;
- Storage of personal information in a cloud storage center outside of Quebec.

Who is it for?

This guide is primarily intended for **privacy officers** in all[2] organizations, and for **members of** public sector **access to information and privacy committees.**

Secondarily, it may also be useful to several other people within:

- **Small businesses**: entrepreneurs, shopkeepers, craftsmen, self-employed workers, association leaders, etc;
- **Large companies**: legal affairs managers, organizational risk management managers, anyone in charge of information systems security, ethics, document management, etc;
- **Public sector organizations:**[3] organizational heads of information security, of document management, of ethics, of information systems development or acquisition, of information security architecture, of service continuity, of information technology management, of physical security, of internal auditing, etc.

---

[1] In this guide, the term "**project**" refers to any project, technological or otherwise, that may involve the collection, use, communication, retention or destruction of personal information.

[2] In this guide, the term "**organization**" refers to private companies and public bodies subject to privacy legislation:
- An **enterprise** is defined as the exercise, by one or more persons, of an organized economic activity, whether commercial in nature or not, consisting of the production or realization of goods, their administration or alienation, or the provision of services (article 1525 of the *Civil Code of Quebec*). It includes a self-employed person, a company, a general or limited partnership, a non-profit organization, a syndicate of co-owners and a union.
- The term "**public bodies**" refers to **government** and **municipal departments** and **agencies,** as well as **health and education organizations**.

The text will be specific when it applies only to one or the other of the sectors.

[3] Job titles may vary.

Is it mandatory to follow the procedure described in this guide?

The law does not specify how a PIA is to be carried out. Nor does it prescribe the content or form of a report on a PIA.

It is not mandatory to follow or apply this guide to the letter.

However, you'll find important pointers to help you structure your PIA process and, where appropriate, your reports.

Introduction

What is a Privacy Impact Assessment?

A PIA[4] is an **approach designed to protect the personal information and privacy of individuals**. It is a form of impact analysis.[5] It evolves over time and must be reviewed throughout the project.

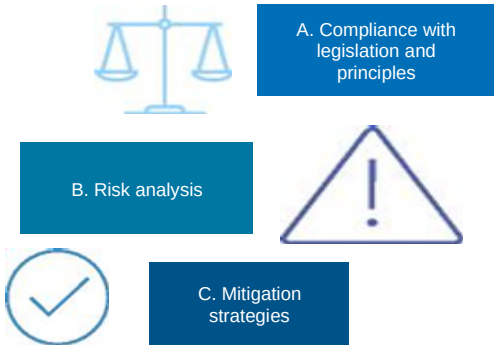
It consists in considering, before starting a project and throughout its duration, **all factors having a positive or negative effect on the privacy of** the people concerned.

These factors are as follows:

A. The project's **compliance with applicable privacy legislation** and **respect for** its supporting **principles;**

B. Identification of privacy **risks** generated by the project and assessment of their consequences;

C. The implementation of **strategies** to avoid these risks or reduce them effectively, and their maintenance over time.



Why perform a Privacy Impact Assessment?

In addition to being mandatory in certain situations provided for by law, the PIA aims to:

- **Protect the individuals** involved in a project, from the collection of their personal information to its destruction;[6]
- **Implement appropriate measures** to comply with your obligations regarding the protection of personal information;
- **Avoid the consequences of** inadequate information management (confidentiality incidents, lawsuits, damage to image or reputation, etc.).

---

4 PIAs are generally referred to as *privacy impact assessments* (PIAs) or *data protection impact assessments* (DPIAs).

5 Like other similar approaches, it enables us to reflect on the impact of a project on a particular area of human life. In spirit, it can be likened, for example, to an environmental impact assessment, an algorithmic impact assessment or a human rights impact assessment. All involve similar steps.

6 Legislation now provides for the possibility of anonymizing personal information instead of destroying it, in certain cases.

When should a Privacy Impact Assessment be performed?

You need to start your PIA **at the very beginning of your project**:

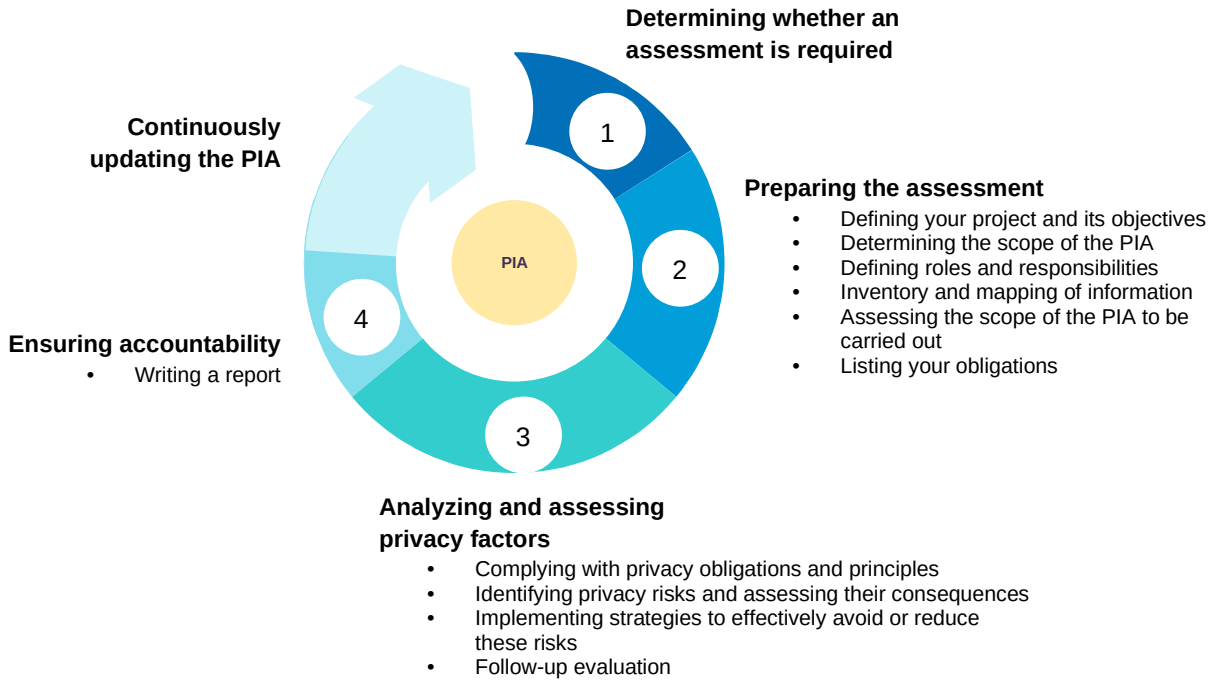
- To be able to influence its progress along the way;
- To act in good time and choose the solution that best protects and respects privacy.

Indeed, to wait before you begin would put you at risk of having to make major changes at a late stage, with all the associated costs and delays. However, it's never too late to start your PIA if you realize it's necessary.

The PIA must evolve throughout the project, according to the changes you make to it. If a PIA has already been produced in the past for the same project, you can update it.

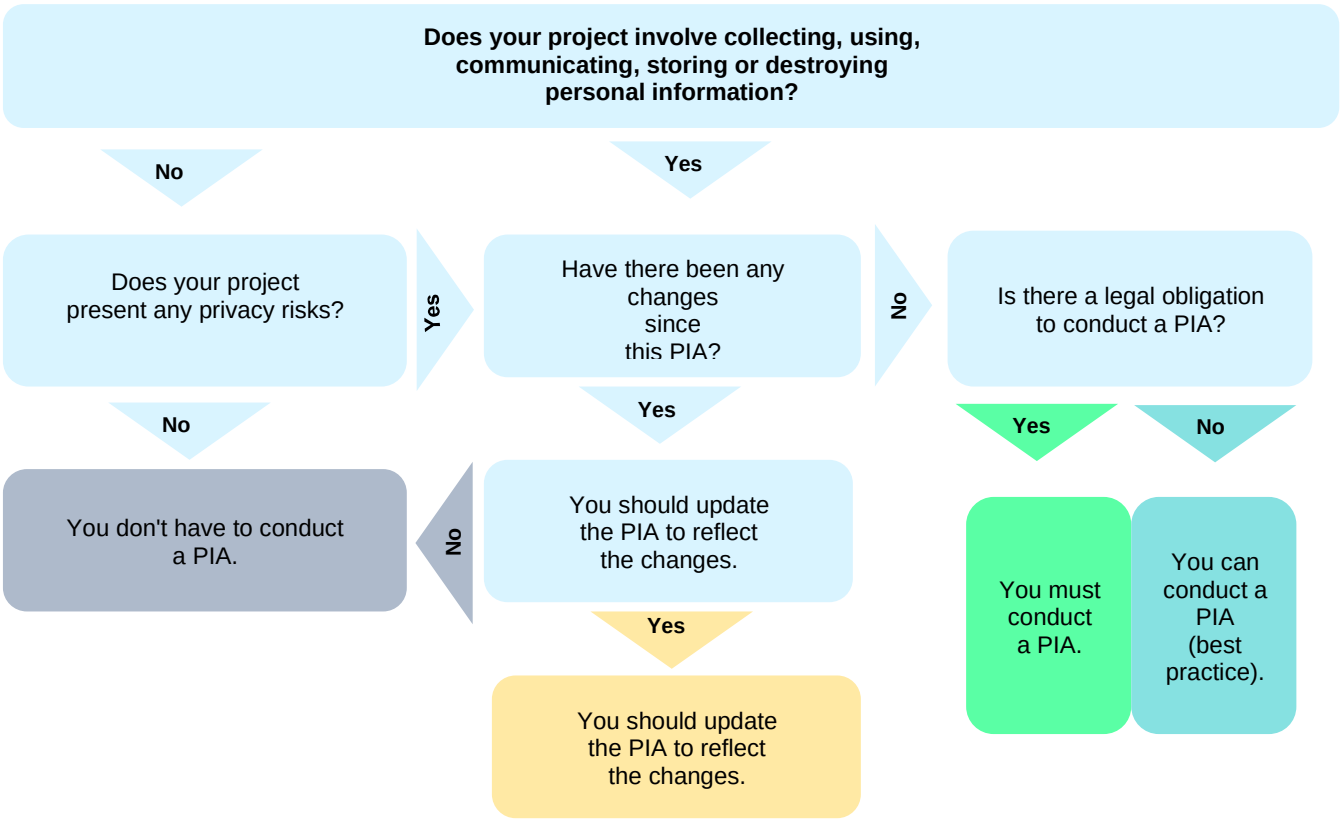
Summary of the PIA process

The rest of this guide is structured according to the stages of the approach proposed by the Commission, presented in the following summary:



1. Determining whether an assessment is required

Before embarking on a PIA process, **check whether it is required.** The following decision tree outlines the questions you need to ask yourself:



As this decision tree illustrates, the key question is: Does your project involve the collection, use, communication, retention or destruction of personal information?

- **If the answer is an unequivocal no**, and your project poses no privacy risk, you don't need to conduct a PIA.

  Caution! Information may, when combined with other information, reveal information about the persons concerned. Don't dismiss the PIA too quickly.

- **If the answer is yes,** a PIA may be required. Continue your analysis:
  - If you **have already carried out a PIA** for a previous version of this project and changes have occurred, you need to update or restart it to take these changes into account.

- If you haven't previously **carried out a PIA** for this project, you should be aware that there are a number of situations that trigger the legal obligation to carry out a PIA. They are set out in the following statutes:

  - *Act respecting Access to documents held by public bodies and the Protection of personal information* ("**Access Act**");
  - *Act respecting the protection of personal information in the private sector* ("**Private Sector Act**");
  - *Act to facilitate the public administration's digital transformation* ("**AFPADT**");
  - *Act respecting the governance and management of the information resources of public bodies and government enterprises* ("**ARGMIR**");
  - Tax Administration Act ("**TAA**").

The following tables show all the situations in which a PIA is **mandatory**, under the legal framework existing at the **date of publication of this guide** (September 22, 2023). Please note that:

- Your analysis must take into account the legal framework specific to your situation. See the details and particularities in the appendices mentioned in the first table;
- The following steps can be applied to any situation;
- If you are not in one of the situations listed in the tables, you can still perform a PIA as a matter of good practice.

1.1. Situations covered by the Access Act and the Private Sector Act

Situation	Articles	Public Sector	Private sector
1. Communication of personal information to a third party, without the consent of the persons concerned, for use in studies, research or the production of statistics Details and special features: appendix 1	67.2.1 - Access Act 21 - Private Sector Act	**Yes**	**Yes**
2. Project for the acquisition, development or overhaul of an information system or electronic service delivery involving personal information Details and special features: appendix 2	63.5 - Access Act 3.3 - Private Sector Act	**Yes**	**Yes**
3. Communication of personal information outside of Quebec	70.1 - Access Act	**Yes**	**Yes**

Details and special features: appendix 3	17 - Private Sector Act		
4. Collection of personal information by a public body on behalf of another body Details and special features: appendix 4	64 - Access Act	**Yes**	**No**
5. Other release of personal information without the consent of the person concerned: a) To another public organization, in Quebec or elsewhere: o To carry out its responsibilities or implement a program under its management; o When the release is clearly to the benefit of the person concerned; b) To any person or organization: o When justified by exceptional circumstances; For the provision of a service to the individual concerned by a public body, in particular for identification purposes Details and special features: appendix 5	68 - Access Act	**Yes**	**No**

There is no obligation to retroactively conduct a PIA under the *Act to modernize legislative provisions respecting the protection of personal information* (Act 25). In other words, if your project was already **finalized on** the date of coming into force of this law[7] (e.g., communication agreement signed, information system implemented, etc.), you are not required to conduct a PIA of the project.

Regardless, you must carry out a PIA:

- **If you modify this project (e.g. amendment to the agreement,[8] system redesign, etc.);**
- **If your project involves the communication of personal information outside of Quebec after September 22, 2023.**

More generally, whenever a project involves personal information, **a PIA is also a good practice.** It can therefore be beneficial to analyze existing systems in the light of new legal obligations.

7 i.e. September 22, 2022 for situation no. 1 and September 22, 2023 for situations n^{os} 2 to 5 in the table.

8 Note that transitional provisions apply for situations n^{os} 4 and 5. See Appendix 4 and Appendix 5.

1.2. Other situations

This guide focuses only on situations covered by the Access Act and the Private Sector Act. Nevertheless, the general approach it presents remains applicable in the following cases:

Situation	Articles	Public Sector	Private sector
6. Information resource project that is of government interest	9 - AFPADT	Yes	No
7. Collection, use or communication for the functions of a public body designated as an official source of government digital data	12.16 - ARGMIR	Yes	No
8. Communication by Revenu Québec to a public body designated as an official source of government digital data	69.1.1 - TAA	Yes	No

2. Preparing your privacy impact assessment

Once it has been determined that a PIA is required, you need to prepare it. You'll need to ask yourself the right questions to identify the aspects of your project that need to be considered, list the personal information involved, assess the scope of the analysis to be carried out, and be aware of the obligations to be met.

2.1. Defining your project and its objectives

First, define your project and the objectives that motivate it.

Outline your project

This step is mainly descriptive. The aim is to document important information that will enable you to assess the risks and the means of eliminating or reducing them (see sections 3.2 and 3.3).

For example:

- What does the project involve?
- What was the context in which the idea for this project came up?
- What is/was the situation when the project started?
- What is the timetable for implementation of the project?

Explain the objectives behind your project

These objectives may explain why you need to implement new measures or practices involving the management of personal information.

An objective must be **legitimate** and relate to **real, serious concerns.**

Examples of project objectives:

- Offering a new public service;
- Deploying an existing service on the Web;
- Increasing safety of a facility;
- Countering fraud;
- Improving detection of a rare health problem;
- Complying with regulations;
- Maintaining your competitiveness;

- Offering a more pleasant customer experience by creating a new version of a platform.

Choose a project that is proportionate to your objectives and the risks of invasion of privacy

You need to assess **proportionality** throughout the PIA process and project implementation.

Proportionality will be observed if:

- There is a rational link between your objectives and the project, i.e. it is an effective means of achieving the objective. This effectiveness must be based on concrete, convincing data;
- The invasion of privacy is minimal, or if there are no other effective, less intrusive solutions;
- The tangible benefits outweigh the consequences or harm for the people concerned.

2.2. Determining the scope of the assessment

By *scope,* we mean what the PIA will cover, its purpose.

What will you include in your PIA?

It's in your interest to clearly define the scope of your PIA, and to keep your analysis at a level appropriate to your project.

Example 1: You decide not to include the revision of identification procedures in your online virtual assistant project. You decide that it doesn't matter, because your current system works well with your in-person and telephone customer service. **Your scope may be too narrow.** Important elements may be missing from your assessment, as online identification may not have the same characteristics as in-person or telephone identification.

Example 2: For the same project, you finally decide to review the identification procedures, the storage of your customer data, the confidentiality forms for your customer service employees and your entire system infrastructure. **Your scope is probably too broad.** Separate assessments could probably be produced for certain sub-processes.

Example 3: For the same project, you're only reviewing your customer service policies and guidelines, without going into the technical details of the software solution you've acquired or the procedures for identifying people. **Your analysis is probably at a level that is too high.** You will miss important elements that exist in the software solution or in the identification procedures.

Example 4: For the same project, separate PIAs have recently been carried out by your organization concerning the procedures and processes for identifying people who contact customer service. **You decide not to redo this part of the analysis, and you analyze only the part that is added concerning identification by the virtual assistant.** You make this clear in your report, so as to inform people of the limits you place on your assessment.

You should be able to justify the scope of your assessment.

→ IF YOU'RE WRITING A PIA REPORT (SEE SECTION 4), THIS STEP AND THE PREVIOUS ONE ALLOW YOU TO INCLUDE:

- The description of the project and its scope.

2.3. Defining roles and responsibilities

The PIA is the responsibility of the organization holding the personal information. It is not the responsibility of any subcontractors, suppliers or partners (e.g. researchers requesting access to the information), even though they may be able to help you in the reflection and analysis of certain aspects.

The law identifies categories or groups of people who must be consulted as part of a PIA:

- At the outset of the project, the public body must consult its **Access to Information and Privacy Committee**, which includes the person responsible for access to and protection of personal information;
- For its part, the company must consult its **Privacy Officer**.

Certain other categories of people may be consulted depending on the scope of the project (see section 2.2) and the scope assessment you have carried out (see section 2.5). These may include, for example, the people in charge of:

- The project;
- Legal affairs;
- Document management;
- Human resources;
- Customer relations.

It can also be:

- Competent authorities within your organization who are required to take a position on risk management at the end of the process (see section 3.4);

- Representatives of the people concerned;
- Your customers or corporate partners;
- Your subcontractors;
- Researchers, etc.

Specify the **roles and responsibilities** of each of the players involved in the assessment, and **when they should be involved** in the PIA process.

For example, some people will need to be consulted from the outset of the project. Others may be consulted at a specific point in the project because of their particular expertise, such as when a privacy issue is identified. Still others may be mandated to monitor the progress of the project and its impact on the privacy of the people concerned.

→ IF YOU'RE WRITING A PIA REPORT (SEE SECTION 4), THIS STEP ALLOWS YOU TO INCLUDE:

- A description of roles and responsibilities.

2.4. Inventory and mapping of personal information

Personal information is at the heart of your assessment. Make an inventory of your personal information, and draw up a map[9] (description, diagram, etc.) that will clearly show the path taken by this information throughout the project.

You'll get the information you need to determine the scope of your PIA. This information will also facilitate your analysis of the project's compliance with applicable legislation and the privacy risks it entails.

appendix 6 provides a list of questions to ask yourself at this stage of the process.

[9] The term *data mapping* is often used.

2.4.1 Taking inventory of personal information

The inventory of personal information enables you to identify its **nature** (e.g. identity, medical, financial information), **sensitivity, quantity** and **purpose.** These concepts are presented in section 2.4.

An inventory is also essential to ensure that you only collect, use or communicate the personal information you need to carry out your project.

However, an exhaustive list of personal information is not required at every stage of the PIA. For example, in the PIA report, a list of groupings of related personal information may suffice.

These groupings contain personal information with common characteristics and/or which, together, allow us to perform a function or achieve an objective.

Your list should still include a short enumeration of the contents of these groupings.

Examples of personal information groupings:

- Customer identity and contact information (first and last name, username, password, etc.);
- Electronic and paper medical records (medical results, appointment summaries, health data, medical imaging, etc.);
- Employee disability files held by human resources (identity information, medical reports, communications with insurers, etc.);
- Call center e-mails and telephone recordings (exchanges with customers, content of questions and answers, voice samples, etc.);
- Website logging data and web analysis tools (history of pages consulted, IP address, browser and device used, display configuration, etc.).

Things to remember

- If you're not sure whether a grouping contains personal information, keep it anyway and consider it in your PIA.
- Include all the information you create or infer about people (credit rating, evaluation score, file note, etc.): this is personal information.
- Think of the information collected automatically by the devices and computer systems you use (device ID, connection logging, etc.).

- Include depersonalized, anonymized and aggregated information[10] in your list. Even if some of this information is no longer directly linked to a person's identity, new technologies often make it possible to re-establish this link. You need to assess the risk of re-identification of this information.
- Even if you only present groupings in the PIA report, it is important for your organization to know the extent of all the personal information it holds.
- The personal information inventory is a living document. Keep it up to date to reflect any changes that may have occurred within your organization (e.g. new collection of personal information for a project). This will enable you to plan your actions properly and meet all your obligations.

2.4.2 Mapping personal information

The mapping of the personal information involved is intended to illustrate its journey through the project, including its **distribution** (between organizations, individuals, systems) and its **storage medium** at each stage of the project. These concepts are presented in section 2.4.

Firstly, in light of your answers to the inventory questions (see section 2.4.1 and appendix 6), identify the **points at which your organization deals or interacts** with personal information.

Interaction points can be:

- **Individuals**, groups of individuals or partners and third parties who access personal information (employees, customers, subcontractors, consulting firms, external researchers, building or computer system maintenance teams, telecommunications providers, etc.);
- **Means** used to **collect** personal information (subscription forms, e-mail inboxes, telephone messaging, collaborative platforms, surveys, questionnaires, etc.);
- **Means** used to **communicate** personal information (electronic service delivery, e-mail exchanges, customer service, Web sites, electronic data interchange interfaces or secure electronic links);
- **Means** used to **process** and **store** personal information (computer systems, cloud services, backup copies, telecommunications tools, paper file storage rooms and filing cabinets, etc.);
- Means used to **destroy** or **anonymize** personal information.

Set out an overview of the flow of personal information throughout your project

Based on the points of interaction you have identified, illustrate the path of personal information through the process covered by your project.

[10] Information is aggregated when several data of the same type are grouped together (e.g. statistics), making it impossible to identify a given individual.

This mapping can take various forms, such as a table, diagram or descriptive text. It will be more complex for larger projects, so a breakdown by process may be preferable in these cases.

Identify the particularities of each phase of your project

The **development phase** of your project may involve privacy risks that are different from those that will exist in the **operational phase**:

- **Development** phase: your project takes shape, you work out solutions to the problems that emerge; people intervene from time to time during this phase (e.g. consultants); you carry out testing on different products; the project may be modified along the way.

- **Operational phase:** your project is alive and kicking, and you're making sure it delivers the results you expect; specific events may occur during this phase, such as system upgrades; employees may leave your company; people may make requests for access to information.

Take this dimension into account when drawing up your information map.

Example 1: I'm the sales manager of a company that produces custom-made clothing. I'd like to make an online ordering tool available to my customers.

A specialized consulting firm will be hired during the **development phase.** I can foresee that these consultants will come into contact with certain information concerning my salespeople and customers throughout the implementation of the system. However, they will no longer have access to this information for a certain period of time after the system goes live, during the **operation phase**. In addition, I have to consider that the risk of computer bugs will be higher during this period. What can I do to reduce the risks?

Example 2: I'm the director of human resources for a large government organization. I'm going to change the human resources management software. The software supplier informs me that the system is updated frequently, and that major upgrades are planned for the coming year. I need to anticipate these possible upgrades during the **operational phase**. I must take steps to ensure that these maintenance operations have no impact on employees' personal data.

→ IF YOU ARE WRITING A PIA REPORT (SEE SECTION 4), THIS STEP ALLOWS YOU TO INCLUDE:

- An overview of the inventory and mapping of personal information.

2.5. Assessing the scope of the PIA to be carried out

If you are legally required to conduct a PIA (see section 1), you must do so, without exception. However, the scope of the PIA may vary depending on the scope of the project, its objectives, the nature of the personal information involved and how it is used and communicated. There may be variations in:

- The number of players involved;
- The amount of time to invest;
- The level of detail of any report (see section 4);
- Ancillary documentation to be prepared;
- The number of measures planned to mitigate or eliminate risks;
- The level of detail of these measures.

Thus, the Access Act and the Private Sector Act provide that the PIA must be proportionate[11] to:

1. The **sensitivity** of the information concerned;
2. The **purpose** of their use;
3. Their **quantity;**
4. Their **distribution;**
5. Their **storage medium.**

It's up to you to determine the scope of your PIA. It's important to document the elements that guide your decision in this regard.

This section offers some non-exhaustive considerations for determining the scope of your PIA.

2.5.1 Assessing the sensitivity of personal information

How **sensitive** is the personal information involved?

Personal information is sensitive when it gives rise to a reasonable expectation of privacy by virtue of its nature or the context in which it is used or communicated.[12]

Examples of sensitive information:

- Ethnicity;
- Information concerning philosophical or religious beliefs;
- Information concerning health or sexual orientation;
- Biometric information;

[11] Access Act, section 63.5; Private Sector Act, section 3.3.

[12] Access Act, section 65.1; Private Sector Act, section 12.

- Some unique identifiers.

Information may also be considered sensitive if it is used in a project specifically affecting a vulnerable population (e.g. minors, ethno-cultural minorities, sexual minorities).

2.5.2 Assessing the purpose of using or communicating personal information

For **what purpose(s)** will personal information be used or communicated? Are these purposes generally risky for individuals? Do they have a significant (e.g. legal) impact on individuals?

Examples of purposes:

- Profiling, locating or identifying a person;
- Systematic or generalized monitoring;
- Establishing a person's profile (consumer, driver, etc.) in combination with other information;
- Making an automated decision about an individual;
- Conducting a study or research or producing statistics;
- Fuelling a new technology with lesser-known effects.

2.5.3 Assessing the amount of personal information

How much personal information will be involved in your project? Does the amount of information involved influence the extent of foreseeable risks?

Examples of questions to ask yourself:

- How many people are affected by your project (absolute number or proportion)?
- What is the volume or scope of personal information involved (all categories combined: collected, observed, inferred, created)?
- How long will the project last? Is it permanent or temporary?
- What is the planned geographical extension?

2.5.4 Assessing the distribution of personal information

How will the personal information involved in your project be **distributed**? Consider the following dimensions in particular:

- **Spatial -** For example, where will personal information be located (within or outside the organization [centralized, decentralized storage])? In which country will the personal information involved in your project be stored?
- **Human or administrative -** For example, to whom will the personal information involved in the project be communicated (e.g., a service provider)?
- **Quantitative -** For example, how many people will have access to this information? How many mediums will it be stored on?

2.5.5 Assessing the medium for storing personal information

On what type(s) of **medium(s)** will the personal information involved in your project be stored, either temporarily or long-term?

This criterion is evaluated according to the nature of the physical or virtual elements used to record, store and consult information.

Examples of medium characteristics:

- Physical (tangible) or digital (e.g. cloud hosting)
- Secured or unsecured
- Connected to other systems or not
- Able to preserve their integrity and confidentiality

→ IF YOU ARE WRITING A PIA REPORT (SEE SECTION 4), THIS STEP ALLOWS YOU TO INCLUDE:

- An overview of the factors justifying the scope of the PIA carried out

2.6. Listing your obligations

Your privacy obligations may come from a variety of sources. This depends on the nature and scope of your project.

Identifying your obligations and understanding the issues involved is no easy task. When in doubt, don't **hesitate to consult a legal expert.**

At the provincial level

In Quebec, the use of personal information is governed mainly by the Access Act and the Private Sector Act.

The following is a non-exhaustive list of other laws that contain specific provisions on the protection of personal information:

- *Quebec Civil Code;*
- *Archives Act;*
- *Act to establish a legal framework for information technology;*
- *Professional Code;*
- *Tax Administration Act;*
- *Highway Safety Code;*
- *Youth Protection Act;*
- *Act respecting health services and social services;*
- *Health Insurance Act.*

Examples of special features and exceptions specified in legislation:

- The collection and use of driver's license and health insurance numbers are governed by laws, regulations or industry directives;
- The management of consent is special for minors and adults lacking legal capacity;
- The collection and use of biometric information[13] is governed in a specific and complementary way by the *Act to establish a legal framework for information technology*.

At the federal and international levels

The federal government and some Canadian provinces have their own privacy laws and regulations. If your company operates in one or more other provinces, make sure you are familiar with the obligations arising from their legislation.

Remember that the communication of personal information outside Québec and Canada is subject to specific provincial and federal legislation.

For international activities, be aware that laws may differ widely from one country to another. What's more, additional obligations may apply to certain categories of personal information, notably sensitive information.

Finally, some legislation is extraterritorial in scope. They apply if an organization collects, uses, communicates or stores personal information about people in the territory covered by these laws, even if the organization is not located in that territory. The European *General Data Protection Regulation* is a case in point. Failure to comply with these laws is sometimes accompanied by significant financial penalties.

[13] For more information, see the *Biometrics* section of the Commission's website.

If your services are aimed at a foreign market or foreign citizens, find out about and consider the effects these laws could have on your project.

Organizational practices

Your organization may manage personal information in a variety of ways, including policies, processes, procedures, work methods, a retention plan and schedule, and so on.

Although such internal documents do not have the force of law, it is important to take them into account in your assessment, so as not to deviate from current practices in your organization. Your work may even enable you to identify shortcomings within your organization.

Standards

There are a number of international standards that can help you reflect on your practices, such as certain ISO standards, or documentation produced by the European Union or the Organisation for Economic Co-operation and Development (OECD). Consult them if you're looking to adopt best practices in terms of privacy and the protection of personal information.

→ IF YOU'RE WRITING A PIA REPORT (SEE SECTION 4), THIS STEP ALLOWS YOU TO:

- Structure your compliance analysis (table, section headings, etc.)

3. Analyzing and assessing privacy factors

This stage is the essential element of the exercise. It involves considering all the factors that will have a positive or negative effect on the privacy of the people concerned.

These factors are as follows:

1. The project's compliance with applicable privacy legislation and adherence to its supporting principles (section 3.1);
2. Identification of privacy risks generated by the project and assessment of their consequences (section 3.2);
3. The implementation of strategies to avoid these risks or reduce them effectively, and their maintenance over time (section 3.3).

3.1. Complying with privacy obligations and principles

To assess the **first privacy factor,** you'll need to **ensure that your project complies with applicable privacy legislation and supporting principles**.

Follow your list (see section 2.6) and assess the extent to which you are meeting your obligations. This may involve legal analyses, documenting certain practices within the company, etc.

Ask yourself the following questions:

- Do you comply with[14] **obligations** and **principles** for the protection of personal information for each category of personal information, at each point of interaction, and throughout the information's life cycle?
- If not, what changes do you need to make to your project to ensure that your obligations and principles are respected?

Document the means you have put in place to comply with your obligations and these various principles. If you have any doubts about your legal obligations, **don't hesitate to consult a lawyer.**

→ IF YOU ARE WRITING A PIA REPORT (SEE SECTION 4), THIS STEP ALLOWS YOU TO INCLUDE:

- A description of the means put in place to ensure compliance with privacy obligations and principles

3.2. Identifying the privacy risks generated by your project and assessing their consequences

[14] For an overview of generally accepted privacy principles, see Appendix 3.

To assess the second privacy factor, you'll need to identify the privacy risks generated by the project and assess their consequences for the individuals concerned.

3.2.1 Identifying the privacy risks associated with your project

What is a privacy risk? A privacy risk is a situation or event that may or may not occur in the future, and that would cause loss or harm to a person's privacy or personal life. Risk is a *potential threat.*

In this case, the loss or damage need not be tangible: the effects of the invasion of privacy may be clear and external (**e.g.**, in the case of damage to the reputation of the persons concerned), or they may be experienced from within by the persons concerned (**e.g.**, a feeling of intrusion).

In this context, certain legally compliant aspects of a project may still be perceived as an invasion of privacy by those concerned.

You therefore need to establish risk scenarios that could arise from the implementation of your project.

Ask yourself the following questions:

- What events or situations can reasonably be expected to occur for each piece of personal information, at each point of interaction and throughout the information's life cycle?
- What are the events or situations that could lead to loss or harm for the persons concerned from the point of view of respect for their privacy?

List the answers you'll give to these questions, and briefly describe the situations.

Examples of privacy risks:

- Excessive collection of information;
- Excessive or unjustified creation of information;
- Lack of information provided to individuals at the time of collection;
- Unauthorized communication of personal information;
- Decision based on inaccurate or ambiguous personal information;
- Theft of personal information;
- Intrusion into private life disproportionate to the purpose of the project;
- Retention of information when its usefulness is no longer proven;
- Re-identification of previously anonymized information.

Your organization may already be in possession of legal opinions or the results of IT security analyses. If non-compliance or information security risks have been addressed in these documents, you can draw on them to produce your PIA.

Describing and assessing potential consequences

Each of these risks can have consequences that need to be described and assessed.

The **potential consequences** are varied:

- Identity theft and fraud;
- Danger to people's lives and safety (such as the possibility of harassment);
- Financial or opportunity losses;
- Damage to reputation;
- Unwanted solicitations;
- Intrusions and other nuisances into people's private lives.

The consequences for your own organization should not be taken into account in the PIA, which aims to preserve the privacy of the individuals concerned. Although these consequences are important, do not consider them in the PIA:

- Potential damage to your organization's reputation;
- Disputes that may arise;
- Potential costs you may incur;
- Etc.

Identifying the causes of these risks

Specify the causes of these situations.

The **potential causes** are equally varied:

- Deficient process;
- Error in handling of information;
- Lack of knowledge or training;
- Insufficient or non-existent monitoring mechanisms;
- Inadequate distribution of responsibilities;
- Malicious behavior;
- Excessive collection of information;
- Faulty or obsolete technologies;
- Unjustified or unnecessary use of sensitive information;
- Absence of consent;
- Insufficient mechanisms to guarantee the accuracy of personal information;
- Existence of a less intrusive alternative that is sufficiently effective to achieve the specified objective.

Taking into account certain particularities

Projects involving new technologies

Certain technologies raise particular issues, and emerging technologies raise questions that are sometimes unprecedented.

To properly assess the risks a technology entails, it's essential to be familiar with it before deploying it, especially if it's never been used before.

The use of biometric data is an example of a technology that raises specific questions and issues.[15] Artificial intelligence, particularly generative intelligence, also comes to mind.

Seek the help of a specialist if you can't make a proper assessment on your own.

Large-scale projects

Large-scale projects often generate greater risks, which can affect a larger number of people.

For projects involving several phases, it may be advantageous or necessary to produce a PIA for each one. The environment and risks of each phase will be different.

For projects that extend over long periods, regular updating of the PIA is essential.

Projects involving ethical issues

Certain types of projects require an assessment by an ethics committee. This is particularly true of scientific research involving humans. These committees sometimes make recommendations related to the protection of privacy. These should normally be taken into account in your assessments (see appendix 1).

Reports on the ethical assessment of new technologies are frequently published by independent organizations or university researchers. These documents often deal with privacy issues. They are relevant sources of information for thinking about the issues and risks generated by technological projects.

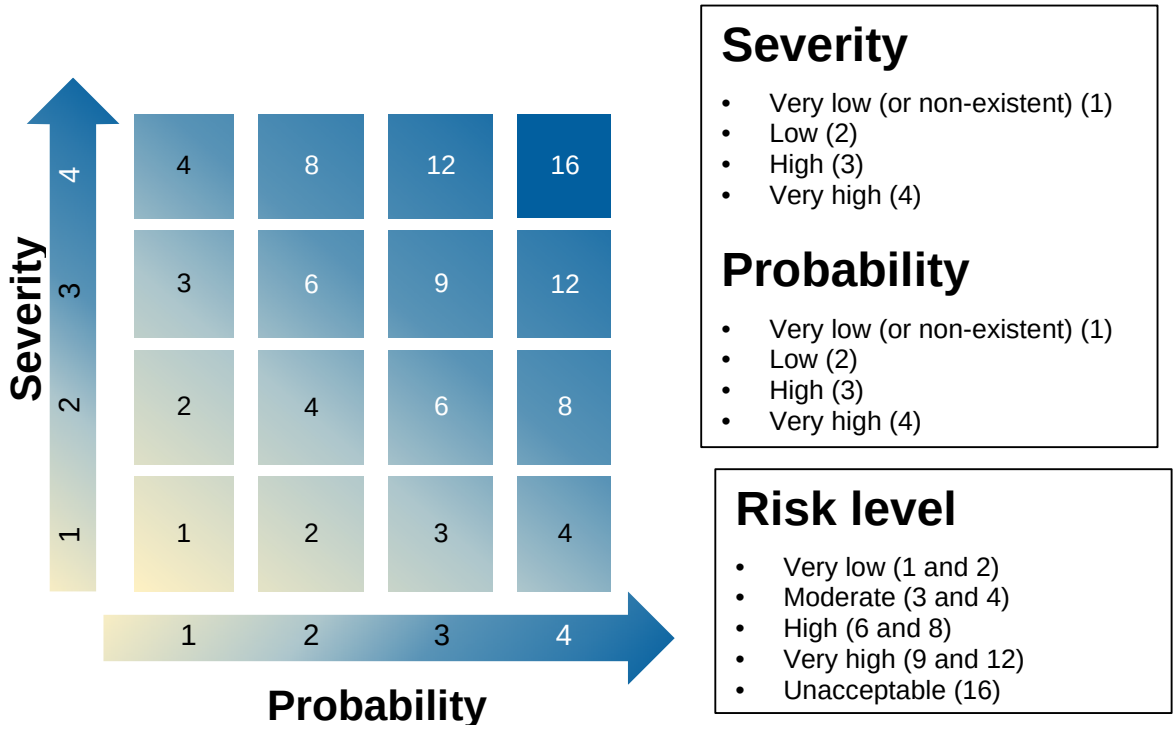
3.2.2 Assessing the level of each identified risk

Devising a method for qualifying risks

There is no prescribed method for qualifying or assessing risks, nor for presenting the results of your analysis. Nevertheless, an assessment based on the **potential severity of an event's consequences**

[15] For information on the use of biometric systems, please refer to the guide produced by the Commission, entitled Biometrics: principles to be respected and legal obligations of organizations (in French).

and the **likelihood of it occurring** can meet PIA objectives. You can, for example, use a rating system and a risk level grid:



Risk assessment is a subjective process. It is often useful to set up a committee to carry out this activity.

If your organization has risk management practices in place, make them a priority.

Assessing the severity of the potential consequences of each identified risk

Severity can be assessed using a rating system.

Example of a rating system to assess **the seriousness of a risk:**

- Very low and/or non-existent (1): the risk entails no consequences for people, or very minor consequences for a single person;
- Low (2): the risk entails minor consequences for one person or a small number of people;
- High (3): the risk has major consequences for one person or minor consequences for a large number of people;
- Very high (4): the risk has major consequences for one person or significant consequences for a large number of people;
- Unacceptable (unrated): the risk generates consequences that are too great and/or involves non-compliance with the law.

Assessing the severity of potential consequences can be influenced by a number of variables:

- The **amount of** information involved;
- The **nature** and **sensitivity** of the information involved;
- The **seriousness** and **nature of the damage** that could be caused (**e.g.** major consequences for the personal or professional life of the people concerned, consequences for their finances, legal procedures or steps they have to take to resolve the situation, danger to their life or safety);
- The **number of people** potentially affected, or their **profile** (**e.g.** children, people with disabilities, immigrants).

Estimating the probability of risks occurring

Your probability estimate can also be made using a rating system.

Example of a rating system to assess **probabilities:**

- Very low and/or non-existent (1): the risk has no chance of materializing;
- Low (2): the risk is unlikely to materialize, or a similar event has never occurred;
- High (3): the risk has a good chance of occurring, or a similar event has already occurred on one or more occasions;
- Very high (4): the risk has a very high probability of materializing, or a similar event has occurred on several occasions.

Considering that zero risk does not exist, this estimate can be very difficult to produce. **Be realistic: avoid being over-confident or over-conservative.**

Estimating the level of risk

Once the severity and probability of the risks have been estimated, you should assign them an overall risk level. If you're using a rating system, a simple way to do this is to multiply the severity rating by the probability rating, as illustrated in the risk level grid on page 23**.**

Considering existing strategies and means of control

Your organization may already have tools, policies, guidelines, procedures or other means in place to mitigate or eliminate risk, but no additional measures have been adopted.

List them and reassess the risks in the light of this information.

Determining the acceptable tolerance threshold for each risk

Put yourself in the shoes of the people concerned, and ask yourself how they might expect their personal information to be used, communicated and protected.

Set yourself thresholds based on what might be acceptable to these people.

You need to establish these thresholds taking into account the context of your project. For example, a person providing medical information has different expectations of a hospital than of advertisers.

→ IF YOU'RE WRITING A PIA REPORT (SEE SECTION 4), THIS STEP ALLOWS YOU TO INCLUDE:

- A risk assessment (events, causes, level of risk)

3.3. Implementing strategies to avoid or reduce risks

To comply with the **third privacy factor,** you'll need to **put in place strategies to eliminate or effectively mitigate the risks** your project poses to the people concerned.

Examining possible strategies to eliminate or mitigate risks

Strategies can seek to reduce either the severity of the potential consequences associated with the risk, or the likelihood of the risk materializing, or both.

Thus, reducing the amount of personal information you collect reduces the potential consequences of data theft. Adding security measures reduces the likelihood of such theft occurring.

Examples of strategies:

- Provide for a periodic review of the various collections of personal information;
- Implement a document management system that enables automated application of the retention schedule;
- Review IT access allocation and management processes;
- Periodically review the security parameters of electronic service delivery;
- Review confidentiality clauses in contracts;
- Establish a schedule of training and awareness-raising activities for your employees;
- Conduct an information campaign about your new use of personal information;
- Keep a log of accesses and use those logs to detect anomalies;
- Depersonalize or anonymize information if its use in a directly identifiable form is not required for everyone.

Choosing the right strategies

Determine what strategies and resources you will put in place to eliminate or mitigate a risk. Consider solutions that are feasible for your organization.

Reassessing the level of each risk

In light of the strategies and resources selected, reassess the level of risk and the likelihood of it occurring.

Check whether you've reached your tolerance threshold. If the threshold has not been reached, re-evaluate your choice of strategy or means.

If, after reviewing your choices, you are still unable to eliminate a major risk, or if your tolerance threshold has not been reached, *you may wish to review this aspect of your project in depth, or withdraw it.*

Any risk that remains at the end, once you've taken steps to reduce or mitigate the risks identified at the outset, becomes a **residual risk.**

Privacy risks may still exist, even after most of them have been eliminated or minimized. If you accept the risks because of their low probability or impact, your organization must nevertheless be able to take responsibility for them.

Even if a risk is completely eliminated, or a strategy is not adopted, you benefit from keeping a record of your approach. This way, your organization can refer to it in the future to understand why you made the choices you did, and avoid having to repeat the whole process unnecessarily.

Reviewing the proportionality of your project

Once you have completed the risk management exercise, repeat the exercise of assessing the proportionality of your project in relation to the risks it still poses to those concerned (see section 2.1).

In light of your PIA as a whole, **does the solution you propose to achieve your objectives still seem proportionate, given the residual risks?**

In the event of a complaint by an individual or an audit by a supervisory body, **will you be prepared to answer the Commission's questions about whether your solution is proportional?**

It may be that the residual risks are too great, and that you need to consider substantial modifications to your project. This may mean starting the PIA all over again, or in part, or even calling the project into question.

→ IF YOU'RE WRITING A PIA REPORT (SEE SECTION 4), THIS STEP ALLOWS YOU TO INCLUDE:

- A description of risk elimination or mitigation strategies

3.4. Following up on your evaluation

Once the privacy factors have been assessed, you should prepare the concrete next step in the PIA. To do this, you should take the following steps.

Drawing up your action plan

The preparation of an action plan ensures that the chosen strategies and resources are implemented.

Integrating the various actions into your day-to-day activities makes the PIA a reality, and enables you to reap the benefits.

Identify those responsible for residual risk management

It is preferable to identify people responsible for monitoring the evolution of residual risks. These people could also be responsible for managing the event, should it materialize.

Inform your leadership

It is important that your organization's senior management is kept informed of the results of the PIA. They must accept both the conclusions of your analysis and the risks that remain despite the means deployed to mitigate them.

→ IF YOU ARE WRITING A PIA REPORT (SEE SECTION 4), THIS STEP ALLOWS YOU TO INCLUDE:

- An action plan

4. Reporting on the assessment

Although it is possible to carry out a PIA without formally documenting it, you should be able to explain and justify your PIA process. Writing a report is a good way to give an account of your thought process when it's complete, or when an important milestone has been reached. If you write a report, you should update it as your PIA progresses.

This report should be simple and accessible: any reader should be able to understand what the project is, how it is likely to affect privacy and how you have considered, measured and mitigated the risks identified.

4.1. What is the purpose of the report?

A PIA report serves to **document and consolidate** the results of your assessment. It provides evidence of your actions and your thought process in the event of an audit, inspection or investigation by a regulatory authority. In addition, when the law requires you to submit a PIA to the Commission, the report is an appropriate means of doing so.

4.2. What should the report contain?

The essentials of your project and its context

- A description of your project;
- What motivated it (context) and its objectives;
- All the parties involved in the project, including a description of their roles and responsibilities: those involved in its implementation and those involved afterwards, i.e. your organization's resources, your various partners and your customers;
- The people or areas of your organization who will be responsible for managing residual risks;
- A summary of consultations, if any;
- An overview of the inventory and mapping of the personal information involved (categories of information involved, source(s) of information, storage medium(s), recipient(s), interactions with other systems, etc.);
- An assessment of the criteria of sensitivity, purpose, quantity, distribution and medium of personal information, and a justification of the depth of analysis (PIA scope);
- A description of the means used to comply with privacy obligations and principles (including sectoral or situational, if necessary);
- A list and categorization of the risks identified for the people concerned;
- The strategies, mechanisms and measures deployed to eliminate or reduce these risks;
- The people responsible for implementing these strategies, mechanisms and measures;
- An action plan with a timetable, including periodic reassessment of the measures put in place (**e.g**. an audit).

A statement that your report has been approved by the highest authorities in your organization

In other words, the details of how the report was approved, including the names, positions and signatures of those who approved it.

Additional information in the form of appendices

- A list of your relevant personal information management and privacy policies;
- A summary of security assessments produced in collaboration with partners or subcontractors (**e.g**. penetration testing);
- Certifications obtained as part of your project (when an assessment body certifies that your product or service complies with certain requirements).

The Commission proposes a generic PIA report template, which you can adapt to your needs. It can take any other form that adequately reflects the process.

4.3. Should the report be distributed?

As a good practice of transparency, your organization may decide to publish an abridged version of the PIA report on its website or by any other means. This can reflect a commitment to comply with the law and for informing those concerned.

Public bodies, in particular, may consider proactively disclosing PIA summaries for projects directly affecting citizens.

→ **TO BE COMPLETED AS REQUIRED**:

- A PIA report

Continuous updating of the PIA

Protecting personal information is not a one-day affair: the PIA is only effective if it evolves continuously, and must be reviewed as necessary, throughout the life cycle of the project.

To ensure the effectiveness of your security measures, you need to monitor their application and revise them according to emerging risks or changes to your project: development of a new business line, plans to implement a service complementary to the transactional system already in place, etc.

Active monitoring tools, such as a security dashboard, will enable you to monitor the consistent and integrated application of the strategies and measures you have put in place.

Appendix 1 - Communication for study, research or statistical purposes

Sections 67.2.1 of the Access Act and 21 of the Private Sector Act

The communication of personal information without the consent of the individuals concerned to a person or organization (hereinafter the researcher) wishing to use this information for study, research or statistical purposes (hereinafter research) is permitted only if a PIA concludes that certain criteria have been met.

Who should carry out the evaluation: the organization or the researcher?

The PIA should be carried out by the organization holding the personal information, based in particular on the information provided by the researcher. For example, the researcher is in a good position to describe how the personal information will be used once it has been communicated, how it is needed for the research, and what security measures are in place.

Please note that the decision of a research ethics committee cannot replace the PIA that must be carried out by the organization holding the personal information. However, its content and recommendations may be useful during the PIA.

How to carry out this PIA?

This PIA can be carried out by following the general approach presented in this guide. However, the PIA should enable you to justify your conclusion as to whether or not each of the five statutory criteria has been met.

1. The objective pursued by the research can only be achieved if the information is commnicated in a form that makes it possible to identify the persons concerned

For example, if it is possible to carry out the research or study using **anonymized information**[16] or synthetic data, the communication of personal information is not authorized.

If the research can be conducted using **depersonalized information,**[17] only this information should be communicated. It is important to note that this information is still confidential personal information. It is up to the researcher to convince you of the need to use personal information, depersonalized or not. The use of non-depersonalized information requires a convincing demonstration of the impossibility of carrying out the research without the “direct identifiers”.

2. It is unreasonable to require the researcher to obtain the consent of the persons concerned with regard to the protection of personal information and their right to privacy

Since this is an exception to the principle of consent, the organization must be able to conclude that it is unreasonable to require the consent of all individuals whose information is required for research purposes. This could be the case, for example, in the following situations. These examples are not exhaustive and, in all cases, must be contextualized in relation to the specific research being evaluated:

- It may be unreasonable to obtain consent from thousands of people whose contact details are not up to date;
- The research could involve information from people who are incapable of consenting or who are deceased;
- The research may rely on depersonalized information held by your organization, making it impossible for the researcher to obtain consent;
- In certain cases, the constitution of a representative sample may require that we do not introduce a bias by using only data from people willing to consent.

3. The objective outweighs, with regard to the public interest, the consequences of the communication and use of personal information on the privacy of the persons concerned

This part of the PIA aims to weigh the public interest purpose of the research against the privacy implications of communicating and using personal information.

This analysis must first identify and describe the various elements and factors to be considered in order to carry out this weighing.

---

16 Information is **anonymized** when it is reasonably foreseeable in the circumstances that, at any time and in an irreversible manner, it will no longer make it possible to identify a person directly or indirectly. Information must be anonymized in accordance with generally recognized best practices and the criteria and procedures determined by regulation. To learn more, consult the *Distinguishing between anonymization and depersonalization* web page (in French).

17 Information is **depersonalized** when it prevents direct identification of the person concerned.

You must then determine whether the public interest objective of the research outweighs its potential impact on the privacy of the persons concerned.

Here are a few examples of questions to ask yourself when evaluating a researcher's request:

- What is the purpose of the research, and why is it in the public interest?
- What are the expected benefits for society?
- What are the different consequences for the privacy of the persons concerned resulting from the communication of their information?
- Can these consequences be minimized in research? If so, how?
- Is the personal information requested sensitive?
- Will the information be linked or compared with other information? If so, what impact will this have on the privacy of the individuals concerned? Will these practices affect the risk of communication of personal information about one or more individuals?
- What makes it possible to believe that the public interest outweighs the consequences of the communication and use of personal information on the privacy of the individuals concerned?

Warning: the assessment of this criterion is not limited to setting out the purpose of the research or simply stating a general effect, such as that it will increase knowledge in a particular field of activity. The expected benefits of the research in relation to the public interest must be specified, and weighed against the consequences for the privacy of the individuals whose information will be used for research purposes.

4. Personal information is used in such a way as to ensure its confidentiality

In this part of the analysis, you need to assess whether the planned use of the information and the various safeguards that will be put in place ensure its confidentiality. Confidentiality must be ensured not only when the information is communicated, but also at all stages of the research. This assessment should take into account the sensitivity and quantity of personal information.

5. Only necessary information is communicated

The PIA must indicate how the organization will ensure that only the information necessary for the research will be communicated to the researcher. Particular attention should be paid to "direct and indirect identifiers" (related to the first criterion, for example: address, full zip code, health insurance number, date of birth or age) and to particularly sensitive information.

What happens after the PIA?

You must enter into a written agreement with the researcher, the content of which is specified in the Access Act and the Private Sector Act. You must then forward it to the Commission. The agreement comes into effect 30 days after it is received by the Commission.

Should a PIA report be sent to the Commission?

Yes, a PIA report is expected (see section 4) to accompany the agreement sent to the Commission. A written document attesting to the PIA process enables your organization to demonstrate that it has met its obligation. It explains how each criterion was analyzed and what elements were considered.

Appendix 2 - Acquisition, development or overhaul of an information or electronic service delivery system

Sections 63.5 of the Access Act and 3.3 of the Private Sector Act

A PIA is required for any **information system or electronic service delivery** project involving the collection, use, communication, retention or destruction of personal information. This may be a project involving:

- Acquisition;
- Development;
- Overhaul.

An **information system** can take many forms. It is not necessarily computerized, although this is often the case. Among other things, it can be a:

- Computerized file processing system;
- Video conferencing or collaboration software;
- Biometric system;
- Artificial intelligence system;
- Chip card/RFID system;
- Video surveillance system;
- Statistical system;
- Payroll management system.

In particular, an **electronic service delivery system** can take the form of:

- A self-service kiosk;
- An RFID/NFC payment service;
- A member area of a website;
- An electronic file;
- A mobile application.

Right to portability of personal information

In addition to conducting a PIA, you must ensure that your project allows computerized personal information collected from the individual concerned to be communicated to them in a structured, commonly used technological format.

As of September 22, 2024,[18] your organization will be obliged, at the request of the person concerned, to provide them with computerized personal information collected from them, in a structured and commonly used technological format.

This communication may also be made to a person or organization authorized to collect the information, at the request of the person concerned.

[18] This obligation, introduced by Act 25, will be incorporated into sections 84 of the Access Act and 27 of the Private Sector Act.

Appendix 3 - Communication of personal information outside of Québec

Sections 70.1 of the Access Act and 17 of the Private Sector Act

A PIA is required:

- Before **communicating** personal information **outside of Québec;**
- Before **entrusting a person or organization outside of Québec** with the task of collecting, using, communicating or storing such information on your behalf.

For the purposes of your assessment, you should consider the following factors in particular:

- Sensitivity of the information;
- The purpose of its use;
- Protective measures, including contractual ones, from which the information would benefit;
- The legal regime applicable in the country where the information would be communicated, in particular the principles of protection of personal information applicable there.

You may communicate information if the PIA demonstrates that the information would benefit from **adequate protection,** particularly with respect to **generally accepted privacy principles.**

What are “generally accepted privacy principles”?

The Access Act and the Private Sector Act do not define “generally accepted privacy principles”.

However, these are general rules designed to ensure the protection of personal information, as well as respect for the rights and interests of those concerned.

Without being exhaustive or definitive, the following list presents principles incorporated into numerous privacy laws and other significant privacy documents, such as standards or guidelines:[19]

- **Accountability**: organizations are accountable for their management of personal information. They put in place policies and practices to protect it, and deploy the financial and human resources necessary to do so, including designating a person to be responsible. They document their compliance and decisions regarding the protection of personal information.
- **Identifying purposes**: the purposes for which organizations collect personal information are legitimate and identified prior to collection.

[19] See in particular the OECD Privacy Guidelines, the U.S. Federal Trade Commission's Fair Information Practice Principles (FIPPs), and the principles underlying legislation such as Canada's *Personal Information Protection and Electronic Documents Act* and the European Union's *General Data Protection Regulation*.

- **Limiting collection**: organizations collect only the information necessary for the purposes identified. Collection is done by fair and lawful means and minimizes invasion of privacy.
- **Consent**: individuals are adequately informed of the identified purposes and freely consent to them, unless an exception applies.
- **Protection by design and by default**: products/services are designed to respect people's privacy. If they include privacy settings, these protect privacy by default.
- **Limiting use, communication and retention**: organizations use and communicate personal information collected for the identified purposes or for compatible purposes, except with consent or legal exception. They limit access to this personal information to authorized persons, and retain it no longer than necessary.
- **Accuracy**: organizations keep personal information up to date and ensure that it is accurate and complete at the time it is used or communicated.
- **Security**: organizations take appropriate security measures to protect the information they hold at all times against loss, theft or unauthorized modification, communication or destruction. These measures are appropriate to the sensitivity of the information and to the context. In the event of an incident, organizations react promptly and notify the persons concerned and the authorities, with certain exceptions.
- **Transparency**: organizations provide relevant information to the individuals concerned at the time of collection or consent. They provide the public with their contact details and clear information on their policies and practices for managing personal information.
- **Individual rights**: individuals can access their personal information and request rectification or, in some cases, deletion. Organizations establish accessible processes to enable the exercise of these rights.
- **Redress**: in the event of dissatisfaction, people can contest a refusal to exercise a right or lodge a complaint with the organization or a competent body.

What is "adequate protection"?

Here again, the Access Act and the Private Sector Act do not define "adequate protection".

This protection can be thought of as offering **legal** guarantees (legislation of the destination jurisdiction) and **contractual** guarantees (agreement with the recipient organization) that comply with all generally recognized protection principles and are appropriate in view of the sensitivity and purpose of the information involved.

If you conclude that personal information will not benefit from adequate protection, you must refuse to communicate it or refrain from entrusting it to a third party outside of Québec.

What must the written agreement following the PIA contain?

Appendix 3 – Communication of personal information outside Québec

Communication of personal information outside of Québec must be subject to a written agreement between you and the third party. This agreement must take into account the results of the PIA. If necessary, it must include agreed-upon terms for mitigating the risks identified in the PIA in order to achieve adequate protection.

Appendix 4 - Collection by a public body on behalf of another public body

Section 64 of the Access Act

A PIA is required when a public body:

- Collects personal information needed to carry out the duties or implement a program of another public body with which it collaborates;
- Collects this type of information to provide services or carry out a joint mission.
    - For example, an organization may collect personal information to verify the eligibility of individuals for a program it administers.

Transitional provisions apply to agreements already in force on the date this PIA becomes mandatory, i.e. September 22, 2023.[20]

Who should carry out the assessment?

It is the organization that will ultimately hold the personal information, i.e., the one that asks another public body to collect personal information on its behalf, that should carry out the PIA, collaborating, where necessary, with the organization assisting it. The latter is well placed, for example, to describe how personal information will be collected, with what security measures, etc.

What happens after the PIA?

Cooperating organizations must enter into a written agreement, the content of which is specified in section 64 of the Access Act. They must then forward the agreement to the Commission. The agreement comes into effect 30 days after receipt by the Commission.

Should a PIA report be sent to the Commission?

Yes, a PIA report is expected (see section 4) to accompany the agreement sent to the Commission. A written document attesting to the PIA process enables your organization to demonstrate that it has met its obligation.

[20] Agreements entered into under sections 64 and 68 of the Access Act before September 22, 2023 remain in force until September 22, 2025, or their expiry date, whichever comes first (section 174 of Act 25). To **renew** or **amend** the agreement, a PIA will now be required.

Appendix 5 - Other types of communication without consent (public sector)

Section 68 of the Access Act

A PIA must also be conducted and conclude that certain criteria have been met before a **public body communicates personal information without consent**:

- To another public organization, in Québec or elsewhere:
  - To carry out its responsibilities or implement a program under its direction;
  - When the commuincation is clearly to the benefit of the person concerned;
- To any person or organization:
  - When justified by exceptional circumstances;
  - For the provision, by a public body, of a service to be rendered to the person concerned, in particular for identification purposes.

Transitional provisions apply to agreements already in force on the date this PIA becomes mandatory, i.e. September 22, 2023.[21]

Who should carry out the assessment?

The PIA should be carried out by **the organization holding** the personal information, in collaboration, where necessary, with the recipient of the communication. The recipient is well placed, for example, to describe how the personal information will be used once it has been communicated, and what security measures will be in place.

How to carry out this PIA?

For these other types of communication to take place, the PIA must allow us to conclude that the following four criteria have been met:

1. The objective can only be achieved if the information is communicated in a form that makes it possible to identify the person concerned

For example, if the purpose of the communication can be achieved using **anonymized information** or synthetic data, the communication of personal information is not authorized.

[21] Agreements entered into under sections 64 and 68 of the Access Act before September 22, 2023 remain in force until September 22, 2025 of their expiry date, whichever comes first (section 174 of Act 25). To **renew** or **amend** the agreement, a PIA will now be required.

If the purpose of the communication can be achieved using **depersonalized information**, only that information should be communicated. It is important to note that this information is still confidential personal information. It is up to the public body to justify the need to use personal information, whether depersonalized or not.

The use of non-depersonalized information requires a convincing demonstration of the impossibility of carrying out the communication without the “direct identifiers”.

2. It is unreasonable to require the consent of the person concerned

Since this is an exception to the principle of consent, you should be able to conclude that it is unreasonable to require the consent of all individuals whose information is required for the purposes of the proposed communication.

3. The objective outweighs, with regard to the public interest, the consequences of the communication and use of personal information on the privacy of the persons concerned

This part of the PIA aims to weigh the public interest purpose of the communication against the consequences of the communication and use of personal information on the privacy of the individuals concerned.

This analysis must first identify and describe the various elements and factors to be considered in order to carry out this weighing.

You must then determine whether the purpose of the communication in terms of the public interest outweighs the possible consequences for the privacy of the persons concerned.

Here are a few examples of questions to ask yourself when evaluating your proposed communication with another public organization:

- What is the purpose of the communication, and why is it in the public interest?
- What are the expected benefits for the people concerned and for society as a whole?
- What are the different consequences for the privacy of the persons concerned by the communication of information?
- Can these consequences be minimized through commuincation? If so, how?
- Is the personal information involved sensitive?
- Will the information be linked or compared with other information? If so, what impact will this have on the privacy of the individuals concerned? Will these practices have an impact on the risks of communicating personal information about one or more individuals?
- What makes it possible to believe that the public interest outweighs the consequences of the communication and use of personal information on the privacy of the individuals concerned?

Thus, the assessment of this criterion is not limited to setting out the purpose of the communication or simply stating a general effect, such as “improved services”. It is necessary to specify the expected benefits of the contemplated communication in relation to the public interest, and to weigh these against the consequences for the privacy of the individuals whose information will be communicated.

4. Personal information is used in such a way as to ensure confidentiality

In this part of the analysis, it is necessary to determine whether the planned use of the information and the various safeguards that will be put in place when it is communicated by the organization ensure its confidentiality. This assessment should take into account the sensitivity and quantity of personal information.

What happens after the PIA?

You must enter into a written agreement with the third party, the content of which is specified in section 68 of the Access Act. You must then forward the agreement to the Commission. The agreement takes effect 30 days after receipt by the Commission.

Should a PIA report be sent to the Commission?

Yes, a PIA report is expected (see section 4) to accompany the agreement sent to the Commission. A written document attesting to the PIA process enables your organization to demonstrate that it has met its obligation. It explains how each criterion was analyzed and what elements were considered.

Appendix 6 - Inventory and mapping of personal information: food for thought

To take inventory of your personal information and map it out, consider the following questions. They can help you map out the path taken by the information identified throughout the project.

Questions	Sub-questions
What?	✓ What **types of** personal **information** will be collected, communicated, used or retained in connection with this project? ✓ What is the nature of this information (e.g. is it **sensitive**)?
Why?	✓ Why do you want to collect, use, communicate or retain personal information? ✓ What is the **purpose of** using this information for your project? ✓ How is access to this information necessary for the performance of the duties of the persons who will have access to it?
How much?	✓ How **much** personal information will be involved in your project? ✓ How many people will be affected by your project (absolute number or proportion)? ✓ What is the volume or scope of personal information involved? ✓ How long is the project expected to last? ✓ What is the planned geographical extension?
Who?	✓ What categories of people will have access to this information within the organization or outside (third parties)?
How?	✓ How or by what means will personal information be collected, used, communicated or stored within (or outside) the organization? ✓ How will the organization dispose of this information once the purpose for which it was collected (or communicated or used) has been achieved? ✓ What method of destruction (or anonymization) will be used?
Where?	✓ Where will this information be **distributed** and stored within (or outside) the organization? ✓ On what type(s) of **mediums** and under what conditions will they be stored?
When?	✓ When will the information be destroyed or anonymized?

Montréal
2045 Stanley Street
Suite 900
Montreal, Quebec H3A 2V4
Telephone: 514 873-4196

Québec
525 René-Lévesque Blvd.
René-Lévesque Est
Suite 2.36
Québec (Québec) G1R 5S9
Telephone: 418 528-7741

Commission d'accès à l'information du Québec

1 888 528-7741 | cai.gouv.qc.ca