Commission d’accès à l’information

Conducting a Privacy Impact Assessment

Guide to the process and its documentation

March 2025

Unofficial translation by BLG LLP

Source: Réaliser une évaluation des facteurs relatifs à la vie privée — Guide d’accompagnement à la démarche et à sa documentation, CAI

Version 3.1 – April 2024

This guide was developed by the *Commission d'accès à l'information* (Commission or CAI) in 2021. It takes into account the *Act to modernize legislative provisions as regards the protection of personal information* (Law 25).

[Original French] version 3.1 has been revised visually and structurally, but the content remains essentially the same.

This guide concerns the Access Act and the Private Sector Act

This guide concerns the *Act respecting Access to documents held by public bodies and the Protection of personal information* (Access Act) and the *Act respecting the protection of personal information in the private sector* (Private Sector Act).

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 its publication. Public and private organizations must comply with the legal framework in force regarding the protection of personal information.

This guide is explanatory and does not replace the law

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

Icons used in this guide

Throughout the guide, you will find four types of information banners, identified by their icon:

- Terminology
- Legal particularity
- Recommendation or best practice
- Warning

The use of the masculine form refers to both men and women, and is used only to lighten the text.

This guide may be reproduced in whole or in part provided that the source is acknowledged, and that it is not used for commercial purposes.

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

If you have any **general questions** about this guide, please contact the Commission. Note that the Commission does not provide legal advice.

Introduction

What is the purpose of this guide?

This guide is designed to help you:

- Determine whether you are obliged to carry out a Privacy Impact Assessment (PIA) for a given project;
- Carry out the PIA;
- Write a PIA report, if required;
  - The guide makes it easier to use the generic report template provided by the Commission (available only in French)

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. Examples include cloud storage of personal information outside of Québec, the purchase of an information system, or a project to communicate personal information to a researcher.

Who is the target audience for this guide?

This guide is primarily intended for those **responsible for the protection of personal information** in all organizations. It is also of interest to **members of a committee on access to information and the protection of personal information** in the public sector.

In this guide, the term "**organization**" refers to private-sector enterprises and organizations (web page available only in French) and public bodies (web page available only in French) subject to privacy legislation.

This guide may also be useful to several other individuals, depending on the case, such as an organization's CEO, in-house counsel, risk management, security, ethics or document management stakeholders, or researchers.

Is it mandatory to follow this guide?

No. The law does not specify how to carry out a PIA, nor does it prescribe the content and form of a report documenting a PIA. It is therefore not mandatory to follow or apply this guide to the letter. However, it does provide important guidelines to help you structure your PIA process and, where appropriate, your report.

What is a Privacy Impact Assessment?

A PIA[1] is a **process that seeks to better protect personal information and ensure that the privacy interests of natural persons are respected**, making it a form of impact assessment.[2] It is an evolving process that needs to be reviewed throughout any project involving the processing of personal information.

It consists of assessing, at the outset of a project and throughout its duration, **all factors having a positive or negative effect on the privacy interests** of concerned persons. These factors are as follows:

A. Compliance with legislation and principles

The project's **compliance** with the applicable legal framework on the protection of personal information and adherence to the principles underlying it.

B. Risk analysis

The identification of privacy **risks** posed by the project and the assessment of their consequences.

C. Mitigation measures

The implementation of **measures** to avoid or effectively reduce these risks, and the maintenance of these measures.

Typically, the PIA is documented in a report, which can be updated as it evolves. The Commission proposes a generic PIA report template (available in French only), which you should consult alongside this guide.

[1] In French, PIA means "Évaluation des facteurs relatifs à la vie privée."
[2] Like other similar approaches, it allows us to reflect on the impact of a project on a particular area of our lives. The intention behind it can be compared, for example, to that of environmental impact assessments, algorithmic impact assessments, or human rights impact assessments. All involve similar steps.

Why conduct a PIA?

The PIA is a **legal obligation in many situations**. It therefore often becomes a question of compliance! It can, however, be carried out as a best practice.

The PIA helps **protect persons** concerned by a project, from the collection of their personal information to their destruction[3]. It also leads to the **implementation of appropriate measures to comply with your obligations** regarding the protection of this information. Finally, it is an important tool to **avoid or mitigate risks** arising from inadequate management of personal information (confidentiality incidents, lawsuits, reputational damage, etc.).

In essence, the PIA is an invaluable tool for reflecting on and demonstrating the **necessity** and **proportionality** of your project, taking into account its objectives and the privacy risks it entails. These two notions are fundamental to the protection of personal information and are **essential conditions of legal compliance**.

If you are unable to justify the necessity and proportionality of your project at the end of the PIA, taking into account the mitigation measures under consideration, you will need to either modify it more substantially or decide to terminate it.

When to carry out a PIA?

You should conduct a PIA at the **outset of your project**:

- To be able to influence its progress along the way;
- To act in a timely manner and adopt the most appropriate solution for protecting and respecting privacy.

Indeed, waiting before you start would put you at risk of having to make major changes late in the process, with the associated costs and delays. However, it is never too late to undertake your PIA if you realize it is necessary.

The PIA must evolve throughout the project, according to any changes you have made. If a PIA has already been carried out in the past for the same project, you can update it.

[3] Legislation now includes the possibility of anonymizing personal information instead of destroying it, in certain cases.

Overview of the PIA process

Step 1

Determine if an assessment is required

Pages 10-13

This step will let you know if you need to carry out an assessment.

Step 2

Define your project and the purpose of the assessment

Pages 14-18

This step will get you off on the right foot by defining your project and deciding what to include in your assessment.

Step 3

Prepare the assessment

Pages 19-30

This step will enable you to map out your personal information, trace its history and determine the breadth of your assessment. You will also need to identify your organization's obligations.

Step 4

Assess privacy factors and adopt appropriate measures

Pages 31-42

This step will enable you to assess your project's compliance and associated risks, and to determine the measures to implement to eliminate or mitigate these risks.

Step 5

Write a report

Pages 43-46

This step will enable you to document your approach and demonstrate compliance with your obligations.

Step 6

Keep the assessment up to date

Page 47

This step will enable you to revise your assessment and keep it up to date over time.

Step 7 | **Particularities in certain situations**

Pages 48-59

Table of contents

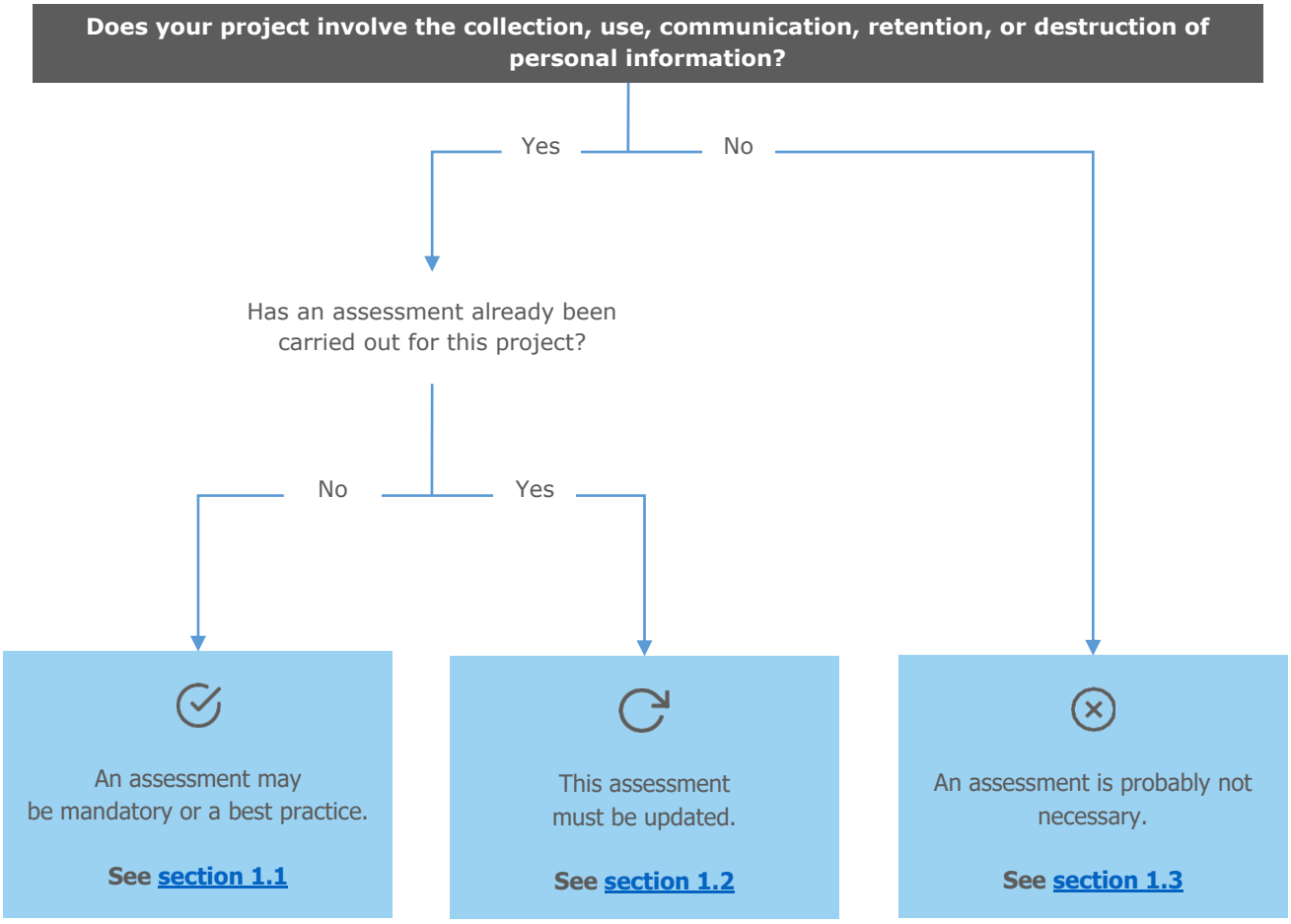
1. Determine if an assessment is required

Before undertaking a PIA, you must assess whether it is required. During this step, you will verify whether your project is subject to a legal obligation to carry out a PIA. If not, you may still choose to conduct a PIA as a matter of best practice.

Include in the summary section of your report:

- **The reason why you are conducting a PIA, with the legal reference, if necessary.**

The first step in the PIA process is to verify whether it is required.



1.1 An assessment is mandatory in five main situations

The following section outlines all situations in which a PIA is mandatory by law, as of the date of publication of this guide (April 2024).

The steps proposed in this guide apply to all these situations. However, your analysis must take into account the legal framework specific to your situation. Details and particularities of each situation can be found in **section 7** of the guide.

The Access Act and the Private Sector Act **require you** to conduct a PIA in five situations.[4]

Situation	Sectors	
	Private	Public
1. You are planning to **communicate personal information outside of Québec.** ✙ **(See section 7.1)** Entry into force: September 22, 2023	Section 17 Private Sector Act	Section 70.1 Access Act
2. You are planning to **acquire, develop, or overhaul an information system or electronic service delivery system involving personal information**. ✙ (**See section 7.2**) Entry into force: September 22, 2023	Section 3.3 Private Sector Act	Section 63.5 Access Act
3. You are planning to **communicate personal information without the consent of the persons concerned** to a person or body **wishing to use the information for study or research purposes, or for the production of statistics**. ✙ (**See section 7.3**) Entry into force: September 22, 2023	Section 21 Private Sector Act	Section 67.2.1 Access Act
4. You are planning to **collect personal information on behalf of another public body** as part of an agreement. ✙ (**See section 7.4**) Entry into force: September 22, 2023		Section 64 Access Act
5. You are planning to **communicate personal information to a person or organization without the consent of the persons concerned** as part of an agreement. ✙ (**See section 7.5**) Entry into force: September 22, 2023		Section 68 Access Act

You must therefore carry out a PIA if:

- You are initiating a new project;
- Your project was not finalized when the PIA requirement came into force;
- You are modifying a project (for example, amendment to the agreement, system redesign, etc.);
- Your project involves the communication of personal information outside of Québec after September 22, 2023.

[4] This guide focuses only on situations covered by the Access Act and the Private Sector Act. Nevertheless, it is applicable to the following situations:
- Information resource project of government-wide interest (section 9 of the *Act to facilitate the public administration's digital transformation*);
- Collection, use, or communication in the exercise of the function of a public body designated as an official source of government digital data (section 12.6 of the *Act respecting the governance and management of the information resources of public bodies and government enterprises*);
- Communication by Revenu Québec (Québec Revenue Agency) to a public body designated as an official source of government digital data (section 69.1.1 of the *Tax Administration Act*).

However, you are not required to carry out a PIA if your project had already been finalized when the obligation came into force.[5] For example:

- The communication outside of Québec had been completed (situation 1);
- The information system had already been implemented (situation 2);
- The communication agreement had already been finalized (situations 3, 4 and 5).

Nevertheless, we recommend that you carry out a PIA:

- If you are not in one of the five situations where a PIA is mandatory;
- If your project was already finalized when the obligation came into force.

Indeed, as soon as a project involves personal information, conducting a PIA is a good practice to protect this information and the privacy of individuals. It may therefore be beneficial to analyze the situation in the light of your legal obligations.

1.2 If you have already conducted an assessment, keep it up to date

If you have already carried out a PIA for an earlier version of your project and changes have occurred, you must **update or start over to reflect these changes**. Take into account the particularities of your situation as detailed in **section 7** of the guide.

1.3 If your project does not involve personal information, an assessment is not mandatory

If your project does not involve personal information and clearly poses no privacy risks, **you do not need to carry out a PIA**. Caution! Some information may, when cross-referenced with other information, reveal information about the individuals concerned. Do not dismiss the PIA too quickly.

If you are not conducting a PIA, we nevertheless recommend that you prepare a very simple report, reflecting your thinking, in which you describe:

- An outline of your project;
- The reason why you are not conducting a PIA.

[5] These dates are listed under each situation on the previous page.

2. Define your project and the purpose of the assessment

Once it has been determined that a PIA is required, you must prepare for it. At this stage, you will need to document the project as a whole and ask yourself the right questions to target the specific aspects of your project that must be considered. You will also need to make an initial assessment of the necessity and proportionality of your project.

With this in mind, you must ensure that the right individuals are involved in the assessment and clarify their responsibilities.

Include in your report:

- **The project description;**
- **The scope of your assessment;**
- **A description of roles and responsibilities.**

2.1 Define your project and its objectives

First, define your project and the objectives behind it.

Describe your project and its context

This stage is primarily descriptive. The aim is to identify important information that will allow you to assess risks and the appropriate measures to avoid or reduce them (see **section 4.2** and **section 4.3**).

For example:

- What does your project involve?
- What was the context when this project was conceived?
- What was/is the situation when the project began/begins?
- What is the implementation timeline?
- How will the project benefit your organization?

Explain the objectives behind your project

These objectives explain why you are initiating the project and why it involves personal information.

Examples of project objectives:

- Offer a new public service;
- Deploy an existing service on the Web;
- Increase facility security;
- Prevent fraud;
- Improve detection of a rare health problem;
- Comply with regulations;
- Maintain your competitive edge;
- Offer a more pleasant customer experience by creating a new version of a platform.

Assess the project's necessity and proportionality from the outset

You must assess **necessity** and **proportionality**[6] throughout the PIA process and the project's implementation. At this stage, you can start thinking about it in a preliminary way by considering the likely risks associated with your project at a high level and in an intuitive way.

[6] To find out more, visit the [CAI] web pages regarding necessity for private-sector enterprises and organizations (available only in French) and government departments and public bodies (available only in French).

The terms "**necessity**" and "**proportionality**" refer to legal concepts of great importance when a project affects a fundamental right, such as the right to privacy.

A project is considered necessary and proportional if:

- The objectives pursued are legitimate, and address important and real concerns;
- There is a rational link between your objectives and the project, in that the latter is an effective means of achieving such objectives. This effectiveness must be based on concrete, convincing data;
- The invasion of privacy is minimal, or if there are no other less intrusive alternative solutions;
- The tangible benefits outweigh the consequences or harm to the persons concerned.

If the necessity and proportionality of your project are uncertain at this stage, the remainder of the PIA will help you gain clarity. You will reassess them at the end of the process, taking into account the measures considered to mitigate or eliminate privacy risks.

Note that a project that is not necessary and proportional is not legal.

2.2 Determine the scope of the assessment

It is in your interest to clearly define the scope of your PIA and to keep your analysis to a level appropriate to your project. You should be able to justify the elements you choose to include in your assessment.

Example 1 – Scope too narrow

You decide not to include the review of personal identification procedures in your online virtual assistant project. You consider this to be of no significance, as your current system works well with your face-to-face 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 – Scope too broad

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 infrastructure. **Your scope is probably too broad.** Separate assessments could probably be carried out for certain sub-processes.

Example 3 – Analysis level too high

For the same project, you are only reviewing the policies and procedures of your customer service department, without examining the technical details of the software solution you acquired or the identity verification procedures. **Your analysis is likely at too high a level.** You will miss important elements that exist at the software solution level or within the identity verification procedures.

Example 4 – Building on pre-existing PIAs

For the same project, separate PIAs have recently been conducted by your organization concerning the procedures and processes for identifying individuals who contact customer service. **You decide not to redo this part of the analysis, and you analyze only the part that is being added concerning identification by the virtual assistant.** You make this clear in your report so as to inform others of any limitations imposed on your assessment.

2.3 Define roles and responsibilities

To ensure the success of your approach, you will generally need to involve other individuals in the assessment. Specify the roles and responsibilities of each of them, and make sure to determine when to involve them.

Who is responsible for carrying out the assessment?

It is the organization that controls the personal information that is responsible for conducting the PIA. It is not the responsibility of any subcontractors, providers, or partners (for instance, researchers requesting access to the information), even though they may assist you in the analysis of certain aspects.

Within the organization, coordination of the PIA may fall on the person responsible for protecting personal information, but it may also be entrusted to or shared with other members of personnel, depending on the project.

Who needs to be involved in the assessment?

Certain individuals must be consulted as part of a PIA:

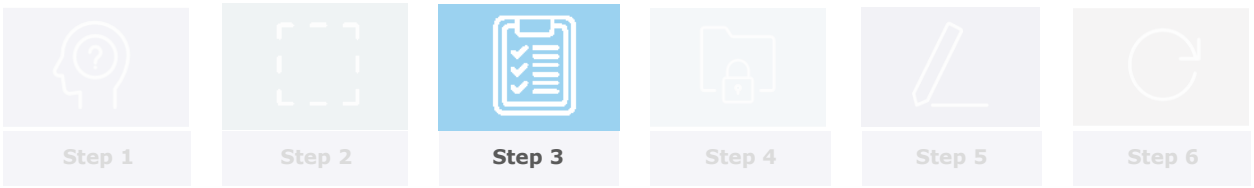
- A public body must consult its **committee on access to information and protection of personal information**, which includes the person responsible for access and protection of personal information, at the very outset of the project;
- For its part, a private-sector enterprise or organization must consult its **privacy officer**.

You may involve certain other individuals based on their specific expertise, depending on the scope of the project (**see section 2.2**) and the assessment of the breadth of the PIA to be conducted (**see section 3.3**). For example, within your organization, you could consult:

- Project leads;
- Individuals responsible for legal affairs;
- Individuals responsible for document management;
- Individuals responsible for human resources;
- Individuals responsible for customer relations;
- The relevant authorities in your organization who will have to adopt a position on risk management at the end of the process (**see section 4.4**).

You may also wish to consult external stakeholders, depending on the context of your project, such as:

- Representatives of the persons concerned;
- Customers or corporate partners;
- Subcontractors;
- A researcher requesting access to the information.



3. Prepare the assessment

Preparing the PIA ensures that you invest your efforts in the right areas and cover the right elements. Since the assessment focuses on personal information, you will first need to know what information your project will involve. You will also need to map its path to understand how it will be exchanged between systems and parties.

This inventory and path will enable you to determine the breadth of the PIA to be carried out, as it must be proportionate to the context: it must be adapted to the sensitivity, quantity, purpose of use, distribution, and medium of the personal information.

Finally, you will draw up a list of your legal obligations to guide you through the assessment itself.

Include in your report:

- **An overview of the inventory of personal information;**
- **A schematic representation of the path of personal information;**
- **The rationale for the breadth of the PIA conducted;**
- **Tables, headings, or analytical tools appropriate to the applicable obligations.**

3.1 Inventory the personal information involved

First, identify all the personal information involved in your project, taking into account the scope of your assessment (**see section 2.2**).

Why make an inventory of personal information?

Your inventory ensures that you collect, use, or communicate only the personal information **necessary** to complete the project.

Even with the consent of the persons concerned, you may not collect personal information that is not necessary for your project. You must be able to demonstrate that the information you collect, use, or communicate is necessary to carry out your project.[7]

The inventory of personal information also allows you to determine:

- Its **sensitivity**;
- Its **quantity**;
- Its **purpose**.

This information will help you assess the breadth of the PIA to be carried out (**see section 3.3**).

[7] For more information on the necessity criterion, see [CAI] pages dedicated to private-sector enterprises and organizations or public bodies and **section 2.1**.

How to structure the inventory?

To structure your inventory, you can answer the following questions:

Questions	Subquestions
What?	• What types of personal information will be collected, communicated, used, or retained as part of this project? • What is the nature of this information? Is it **sensitive** because of its nature or the context of its use?
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 will individuals with access to the personal information need it to perform their duties?
How much?	• What **quantity** of personal information will be involved in your project? • How many individuals will be affected by your project (absolute number or proportion of the population concerned)? • What is the volume or breadth of personal information involved? • What is the planned duration of the project? • What is the geographical scope of the project?

Remember to include in your inventory **all the information involved**, including:

- Information you **create** or **infer** from other information, such as a credit rating or interest profile;
- Information **automatically collected** by devices and information systems, such as a device identifier or connection history;
- Information that is **grouped together** (also called aggregated information), even if it can no longer be used to identify a given individual, such as statistics;[8]
- Information that no longer directly or indirectly identifies an individual (that is, **de-identified** and **anonymized** information).[9]

[8] You need to assess the risk of re-identification of aggregated, de-identified, or anonymized information, that is, the risk that the information will be traced to the person concerned. New technologies often make this possible. For more information, please consult the [CAI] web pages on de-identification and anonymization for private-sector enterprises and organizations, and for government departments and public bodies.

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

How to group personal information?

An exhaustive list of personal information is not required at every stage of the PIA. For example, a list of groupings of related personal information may be sufficient in your PIA report. However, even if you present groupings, you must still be able to know the breadth of the personal information involved in the project.

You can group personal information in different ways. For example, you could group information that:

- Shares common characteristics;
- Serves the same function or achieves the same objective.

If you are not certain whether a grouping contains personal information, you should retain it and consider it for your PIA.

Note that a list should still include a short enumeration of the contents of these groupings. In the examples below, this is shown in parentheses.

Examples of groupings:

- Identity and contact information (last name, first name, username, password, etc.);
- Medical records, both electronic and paper (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 centre emails 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.).

When should the inventory of personal information be updated?

The inventory of personal information is a dynamic process. Keep it up to date to reflect any changes that may occur within your organization (for example, a new collection of personal information for a project). This way, you will be able to properly plan your actions and meet all your obligations.

3.2 Map the path of the personal information

Once you know what information is involved in your project, you must map its path.

> The term "**path**" refers to a structured representation or description of the stages in the processing of information, from collection to destruction, specifying the organizations, persons, systems, and media involved. This is sometimes referred to as "data mapping" or "data flow diagram."

Mapping of personal information allows you to specify, among other things:

- **Distribution**;
- **Medium**.

This information will help you assess the breadth of the PIA to be carried out (**see section 3.3**).

Identify the points of interaction with personal information

First, based on your inventory (**see section 3.1**), identify the **points where your organization (or another organization or person) interacts** with personal information. Points of interaction can be:

- **Persons**, sets of persons, or partners and third parties who access personal information (employees, customers, subcontractors, consulting firms, external researchers, building or information systems maintenance teams, telecommunication providers, etc.);
- **Means** used to **collect** personal information (subscription forms, email boxes, telephone messaging, collaborative platforms, surveys, questionnaires, etc.);
- **Means** used to **communicate** personal information (electronic service delivery, email exchanges, customer service, websites, computerized exchange interfaces [APIs], or secure electronic links);
- **Means** used to **process** and **store** personal information (information systems, databases, cloud services, backup copies, telecommunications tools, storage rooms and filing cabinets for paper documents, etc.);
- Means used to **destroy** or **anonymize** personal information.

To help you, you can answer the following questions:

Questions	Subquestions
Who?	• What categories of persons will have access to personal information within the organization or outside (third parties)?
How?	• How or by what means will personal information be collected, used, communicated, or retained 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 **medium** and under what conditions will it be stored?
When?	• When will the information be destroyed or anonymized?

Mapping the path of personal information throughout the project

Based on the points of interaction you have identified, illustrate how personal information flows throughout the process covered by your project.

This can take various forms, such as a table, a schematic representation of the process, or a descriptive text. Below is an example of a table used to illustrate a path in a simple project:

Information or information grouping	Collection (responsible individuals, source, time, place, means...)	Use (responsible individuals, time, time, place, means, purposes...)	Communication (responsible individuals, recipients, situations, means, reasons...)	Retention (responsible individuals, means, duration, place)	Destruction (responsible individuals, time, place, means, trigger)
Grouping 1					
Grouping 2					
...					

You could also prepare a table specifying the persons and organizations that will have access to the information during its life cycle, indicating the type of access and the reasons justifying this access.[10]

[10] The generic report template proposed by the Commission contains an example of such a table in section 3.

The path will be more complex for larger projects, so a breakdown by process may be preferable in these cases.

For instance, 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 is in progress, and you are working on solutions to emerging problems; individuals intervene from time to time during this phase (for instance, consultants); you carry out trial runs on different products; the project may be modified along the way.
- **Operational** phase: your project is alive and kicking, and you are making sure it delivers the expected results; events may occur specifically during this phase, such as system updates; employees may leave your organization; individuals may submit access to information requests.

If your project includes such phases, and they are clearly distinct in terms of personal information management, you should represent how information flows separately for each of these phases.

Example 1: You are the sales manager of a company that manufactures custom-made clothing. You would like to make an online ordering tool available to your customers. A specialized firm will be hired during the **development phase**. You must anticipate that these consultants will have access to certain information about 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 has been installed, during the **operational phase**. In addition, you must consider that the risk of computer errors will be higher during this period.

Example 2: You are the director of Human Resources at a large government organization. You are changing the Human Resources management software. The software provider informs you that the system is updated frequently, and that more major overhauls are planned for the coming year. You must anticipate these possible overhauls during the **operational phase**. You must take steps to ensure that these maintenance operations have no impact on employees' personal information.

3.3 Assess the breadth 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 breadth of the PIA may vary depending on the scale of the project, its objectives, the nature of personal information involved, and how it is used and communicated. There may be variations in:

- The number of parties involved (**see section 2.3**);
- The time to invest;
- The level of detail of a report (**see section 5**);
- The supporting documentation to be produced;
- The number of measures designed to mitigate or eliminate risks (**see section 4.3**);
- The level of detail of these measures.

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

1. The **sensitivity** of the information concerned;
2. The **purpose** for which it is to be used;
3. The **quantity** of information;
4. The **distribution** of information;
5. The **medium** on which the information is stored.

It is up to you to determine the breadth of your PIA. It is important to record the elements that guide your decision in this regard.

Without being exhaustive, this section offers some food for thought in determining the breadth of your PIA. The inventory (**see section 3.1**) and mapping of personal information (**see section 3.2**) that you prepared should greatly assist you in this reflection.

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

Assess the sensitivity of personal information

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

Personal information is sensitive if, due to its nature or the context of its use or communication, it entails a high level of reasonable expectation of privacy.[12]

Examples of sensitive information:

- Information concerning ethnicity;
- Information concerning philosophical or religious beliefs;
- Information concerning health or sexual orientation;
- Biometric information;
- Certain unique identifiers.

Information may also be considered sensitive if it is used in a project specifically affecting a vulnerable population (for example, minors, ethnocultural minorities, or sexual minorities).

Assess the purpose of using or communicating personal information

For **what purpose(s)** will personal information be used or communicated? Are these purposes generally considered harmful to the persons concerned? Do they have a significant (such as legal) impact on them?

Examples of purposes:

- Verify the identity of clients when they wish to access their file, or carry out transactions;
- Calculate and issue employee pay;
- Establish an individual's profile (for instance, consumer or driver profile, etc.) in combination with other information;
- Render an automated decision about a person;
- Conduct a study or research project, or produce statistics;
- Improve an artificial intelligence model.

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

Assess the quantity of personal information

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

Examples of questions to ask yourself:

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

Assess 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 (for instance, a service provider)?
- **Quantitative**. For example, how many individuals will have access to this information? On how many media will it be stored?

Evaluate the medium for storing personal information

What type(s) of **media** will be used to view, record, or consult the personal information involved in your project, either temporarily or long term?

Examples of media characteristics:

- Physical (tangible) or digital (such as cloud storage);
- Secure or non-secure;
- Connected to other systems or not.

3.4 List your obligations

In order to assess the first privacy factor, it is advisable to draw up a list of your obligations regarding the protection of personal information at the outset. Depending on the nature and scope of your project, these obligations may stem from different sources.

Identifying your obligations and understanding the issues involved can be a complex task, especially if your project itself is complex. In doubt, we **recommend that you consult a lawyer**.

Provincial obligations

In Québec, the protection of personal information is mainly governed by the Access Act and the Private Sector Act. General information regarding the obligations under these laws can be found on the Commission's website in the appropriate sections (available in French only):

- Government departments and public bodies;
- Private-sector enterprises and organizations.

These sections are organized around the life cycle of personal information, from collection to destruction, and present transverse obligations relating to responsibility, consent and security.

The term "**life cycle**" refers to all the phases through which personal information undergoes within an organization.[13] These phases are collection, use, communication, retention and destruction. Each phase is associated with specific obligations for the organization.

You may also have to apply obligations forest out in other laws or regulations. For assistance, please consult those listed on the Commission's website (available in French only).

Examples of particularities and exceptions specified by statute:

- The collection and use of driver's license numbers and health insurance numbers are governed by sector-specific laws, regulations or directives;
- The collection and use of biometric information[14] are governed in a specific and complementary manner by the *Act to establish a legal framework for information technology*.

[13] For more information, please consult the [CAI] life cycle web pages for private-sector enterprises and organizations, and for government departments and public bodies (available in French only).
[14] For more information, see the Biometrics section (available in French only) on the Commission's website.

Finally, depending on the reason for conducting a PIA (**see section 1.1**), you may need to ensure that your assessment allows you to meet specific criteria, or provide for entering into a formal agreement. Be sure to include these obligations in your list.

For more information on the particularities associated with each of the five situations requiring a PIA in the Access Act and the Private Act, **see section 7**.

Federal and international obligations

The federal government and some Canadian provinces have their own laws and regulations regarding the protection of personal information. If your enterprise or organization operates in one or more provinces, make sure you are familiar with the obligations arising from their legislation.

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

For international activities, you should be aware that laws can differ greatly from one country to another. Moreover, additional obligations may apply to certain categories of personal information, notably sensitive information.

Finally, certain laws apply if an organization collects, uses, communicates, or retains the personal information of individuals located in the territory covered by these laws, even if the organization itself is not located in that territory. The European *General Data Protection Regulation* is one example. Failure to comply with these laws can sometimes result in heavy financial penalties.

If your services target foreign markets or citizens, inform yourself and consider the effects these laws could have on your project.

Organizational practices

Your organization may regulate the management of personal information in a variety of ways, including through policies, processes, procedures, work practices, a retention plan and schedule, etc.

Although such internal documents do not carry any legal authority, it is important to take them into account in your assessment, so as not to deviate from your organization’s current practices. Your work may even allow you to identify gaps within your organization.

Standards

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

4. Assess privacy factors and implement appropriate measures

You have now described your project and the scope of the assessment, identified the individuals and organizations that must be consulted, prepared an inventory of the personal information involved, mapped its path, determined the breadth of the PIA to be conducted, and identified your obligations. You are now ready to analyze, in detail, the privacy factors, that is, all those that will have a positive or negative effect on the protection of concerned persons' privacy.

During this stage, you will assess whether your project includes all necessary measures to comply with the applicable laws and principles governing the protection of personal information. You will also consider the potential risks to the persons concerned according to your project and determine strategies (legal, technical, administrative, etc.) to mitigate or eliminate these risks.

Taking into account both the measures already in place and those planned, you will then reassess any residual risks and, consequently, to what degree the principles of necessity and proportionality are respected, in order to decide on the next steps for the project. If you are able to proceed with its implementation, you will then develop an action plan to operationalize the strategies identified in your assessment.

Include in your report:

- **A description of the measures implemented to comply with privacy laws and principles;**
- **A demonstration that the specific criteria the PIA must address have been met, where applicable;**
- **A risk assessment (events, causes and consequences, level of risk);**
- **A description of the strategies required to eliminate or mitigate the risks;**
- **An action plan to implement these strategies.**

4.1 Respect your obligations and personal information protection principles

To assess the first privacy impact factor, you will need to ensure that your project complies with applicable laws and principles governing the protection of personal information.

Follow your list (**see section 3.4**) 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:

- Are you complying with your **obligations** and **principles**[15] governing the protection of personal information for each category of personal information, at each point of interaction, and throughout the information life cycle?
- Can you demonstrate that you comply with the **specific criteria** associated with the legal situation that is leading you to carry out a PIA, if applicable (**see section 7**)?
- If not, what changes need to be made 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 whether your legal obligations have been met, do not hesitate to consult a lawyer.

4.2 Identify the privacy risks associated with your project and assess their consequences

To assess the second privacy impact factor, you will need to identify the privacy risks associated with the project and assess their consequences for the persons concerned.

Identify the privacy risks associated with your project

Wherever personal information is involved in a project, it necessarily presents privacy risks to the persons concerned.

[15] For an overview of generally accepted personal information protection principles, please consult **section 7.1**.

The term "**privacy risk**" refers to a situation or event that could cause harm to an individual's privacy, or to another right still in relation to the individual's privacy. This risk is a *potential threat* to the right to privacy, likely to materialize in the future.

Risks may arise from non-compliance with the law, but also from external action (such as a cyberattack). They may also arise if individuals' reasonable expectations regarding privacy are not respected. **Note that certain aspects of a project that are legally compliant may still be perceived as a privacy breach by the persons concerned.**

To establish risk scenarios associated with your project, ask yourself the following questions:

- What are the **events** or **situations** that could reasonably arise for each piece of personal information, at each point of interaction, and throughout the information life cycle?
- What events or situations could result in losses or harm to the persons concerned, from a privacy point of view?

List the answers you will provide to the above questions and briefly describe these situations.

Examples of privacy risks:

- Excessive collection of information;
- Excessive or unjustified creation of information;
- Lack of information provided to the persons concerned at the time of collection;
- Unauthorized communication of personal information;
- Decision based on inaccurate or incomplete personal information;
- Theft of personal information;
- Disproportionate privacy intrusion for the purpose of the project;
- Retention of information when no longer needed;
- Re-identification of previously anonymized information.

Your organization may already be in possession of legal opinions or IT security analysis results. If non-compliance or security risks have been addressed in these documents, **we recommend that you draw on them to produce your PIA.**

Describe and assess potential consequences of each risk

Specify the potential causes of the identified risks in the context of your organization. Note that the same risk may be caused by multiple factors.

Examples of causes:

- Deficient process;
- Errors in handling information;
- Lack of knowledge or training;
- Insufficient or non-existent monitoring mechanisms;
- Inadequate distribution of responsibilities;
- Malicious behaviour;
- Excessive collection of information;
- Faulty or outdated technologies;
- Unjustified or unnecessary use of sensitive information;
- Lack of consent;
- Insufficient mechanisms to guarantee accuracy of personal information;
- Existence of a less intrusive yet efficient alternative means of achieving the identified objective.

Each of these risks could have consequences for the persons concerned. Describe and assess the potential consequences for individuals' rights.

A consequence need not be tangible to be considered: it may be apparent and external (like in the case of reputational damage to the persons concerned), or it may be experienced internally by the persons concerned (such as a feeling of intrusion). Similarly, it may be associated with an invasion of privacy but concern other individual rights, such as the right to autonomy or freedom of expression.

Beware! Depending on the breadth of your PIA, you should also consider consequences that seem relatively minor, especially when they are likely to be experienced by a large amount of people. Indeed, a minor individual harm can take on great importance when considering its effect on a group of individuals.

Examples of consequences:

- Identity theft and fraud;
- Dangers to individuals' lives and safety (such as the possibility of harassment);
- Loss of autonomy (for example, manipulation);
- Financial or opportunity losses;
- Discrimination;
- Reputational damage;
- Psychological distress;
- Self-censorship due to a deterrent;
- Unwanted solicitation;
- Intrusions and other nuisances into individuals' private lives.

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

- Potential damage to your organization's reputation;
- Potential litigation;
- Potential costs you may incur, etc.

Take into account certain particularities

When identifying risks, their causes, and their potential consequences, take into account the context of your project, particularly if it involves new technologies, is large scale, or has ethical implications.

Projects involving new technologies

Some technologies raise special issues, and emerging technologies sometimes pose unprecedented questions.

To properly assess the risks associated with a technology, it is essential to be familiar with it prior to deployment, especially if it has never been used before.

The use of biometric data is an example of a technology that raises particular questions and issues.[16] Artificial intelligence, especially generative AI, also comes to mind.[17]

Ask a specialist for help if you cannot carry out an adequate assessment on your own.

[16] For more 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.
[17] For more information on the use of generative artificial intelligence, please refer to the position paper drawn up by the Commission and its Canadian counterparts.

Large-scale projects

Large-scale projects often generate more risks, which may affect a greater number of individuals.

For projects involving several phases, it may be advantageous or necessary to produce a PIA for each phase (**see section 3.2**). The environment and risks will differ between phases.

For projects lasting 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 relating to the protection of privacy. These should normally be taken into account in your evaluations (**see section 7.3**).

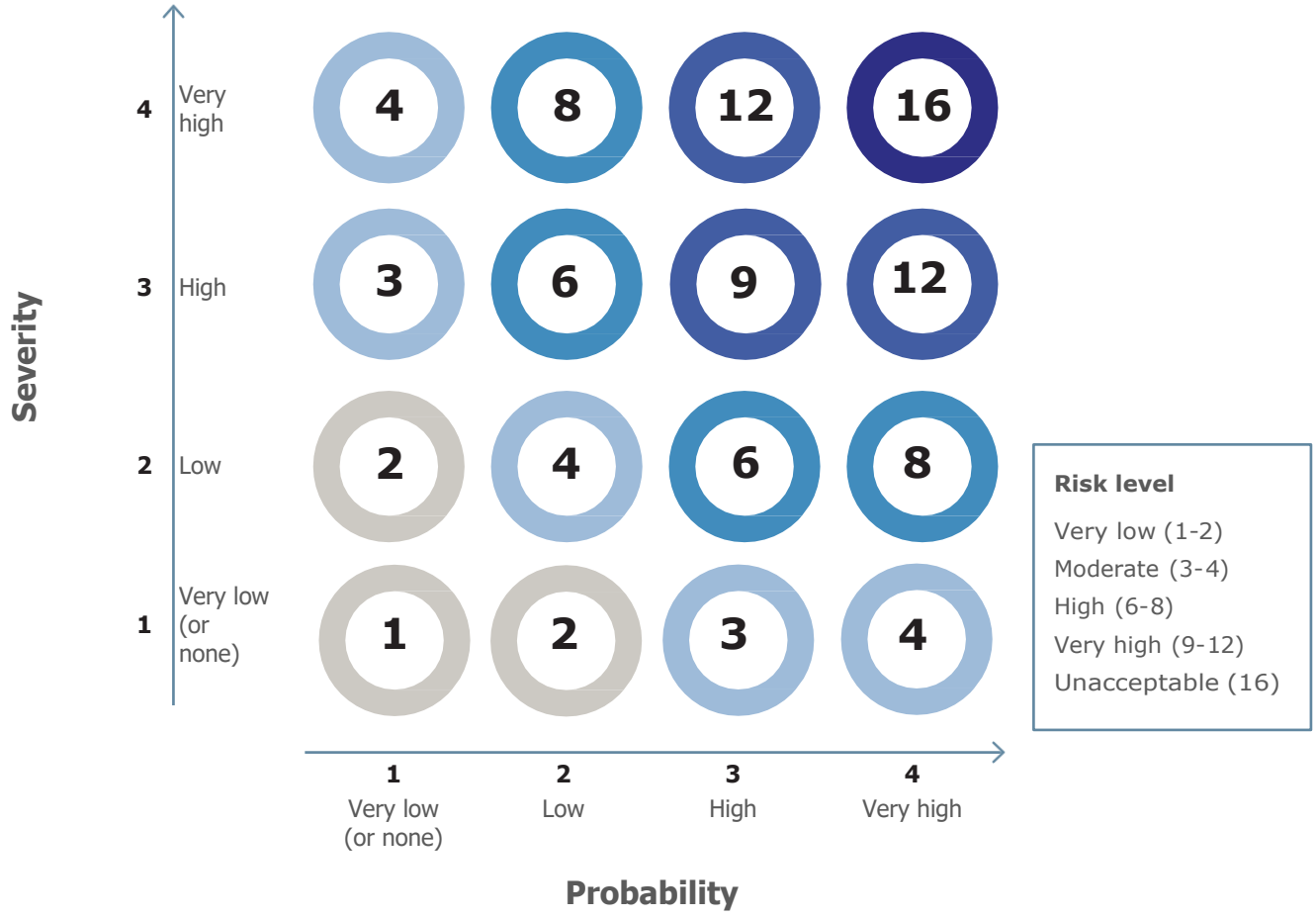
Reports on the ethical assessment of new technologies are frequently published by independent organizations, such as the *Commission de l'éthique en science et en technologie* (Commission on Ethics in Science and Technology) (available in French only), or university researchers. These documents often deal with privacy-related questions. They are relevant sources of information for assessing the issues and risks associated with technological projects.

Assess the initial level of each identified risk

To get an initial picture of the extent of the risks associated with your project, assess their level. This will guide you in selecting mitigation strategies and give you a useful baseline against which to assess their potential effectiveness.

Adopting a method for qualifying risks

The law does not prescribe a 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** and **likelihood** can meet the PIA objectives. For example, you can use a rating system and a risk level grid, such as the graph below:



Assessing the level of risk is a subjective process. It is often useful to set up a committee to carry out this activity.

If your organization already has risk management practices in place, **we recommend that you make them a priority**. You will then be able to rely on methodology that has been tried and tested in your context.

Assess the severity of the potential consequences of each identified risk

The first component of risk level is the severity of the consequences that could affect the persons concerned if it were to occur. Assessing the severity of the potential consequences can be done using a rating system.

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

- **Very low and/or non-existent (1)**: the risk entails no impact on individuals, or very minor consequences for a single individual;
- **Low (2)**: the risk has minor consequences for a single individual or a small number of individuals;
- **High (3)**: the risk entails major consequences for an individual or minor consequences for a large number of individuals;
- **Very high (4)**: the risk has major consequences for an individual or significant consequences for a large number of individuals;
- **Unacceptable (not rated)**: the risk generates consequences that are too great and/or involve non-compliance with the law. If you identify a risk of this level of severity, you must eliminate it before you can proceed with your project.

Certain variables, including those you considered when determining the scope of the PIA (**see section 3.3**), may influence the severity of potential consequences. In particular, consider:

- The **quantity** of information involved;
- The **nature** and **sensitivity** of the information involved;
- The **nature of the harm** that could be caused (**examples**: major consequences for the personal or professional lives of the persons concerned, consequences for their finances, legal procedures or steps they must take to resolve the situation, or danger to their life or safety);
- The **number of persons** potentially affected, or their **profile** (**examples**: children, individuals with disabilities, immigrants).

Estimate the probability of risks occurring

The second component of the level of risk is the probability of a risk occurring. The probability can also be assessed 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 has little chance of materializing, or a similar event has never occurred;
- **High (3)**: the risk has a good chance of materializing, 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.

Given that there is no such thing as zero risk, this estimate can be very difficult to produce. **We recommend that you be realistic: avoid being overconfident or over-conservative.**

Estimate the level of risk

Once the level and probability of risks have been estimated, you should assign them a global risk level. If you are using a rating system, a simple way of doing this is to multiply the level of risk by the level of probability, as illustrated in the risk level grid on **page 37**.

Consider existing measures and controls

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

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

Determine the acceptable tolerance threshold for each risk

Put yourself in the shoes of the persons concerned and ask yourself how they might expect their personal information to be protected when it is:

- Collected;
- Used;
- Communicated;
- Retained;
- Destroyed.

Set thresholds for what might be acceptable to them.

These thresholds should be established according to your project's circumstances. For example, an individual providing medical information has different expectations towards a hospital than towards advertisers.

4.3 Implement strategies to prevent or reduce risks

To comply with the third privacy factor, you will need to put in place strategies to effectively prevent or reduce the risks your project poses to the persons concerned.

Examine possible strategies and select the best

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

Hence, reducing the quantity of personal information you collect reduces the potential consequences of data theft. Rather, adding security measures reduces the likelihood of such theft occurring.

Your strategies may be legal or administrative, physical or technical.

Examples of strategies:

- Plan a periodic review of the various collections of personal information;
- Implement a document management system that enables automated application of the retention schedule;
- Review computer access allocation and management processes;
- Periodically review security parameters for electronic service delivery;
- Review confidentiality clauses in contracts;
- Establish a training and awareness schedule for your employees;
- Restrict access to premises where documents containing personal information are kept;
- Conduct an awareness campaign about your new use of personal information;
- Log access and use logs to detect anomalies;
- De-identify or aggregate information if using it in a directly identifiable form is not required for all data.

From the range of measures considered, determine which ones you will put in place to reduce or eliminate a risk. Think of solutions that remain feasible for your organization.

Reassess the level of each risk

In light of the measures and means adopted, reassess the level of risk by reconsidering the severity of the consequences and the likelihood of it occurring. Once again, follow the steps outlined in **section 4.2**.

Verify whether you have reached the tolerance threshold set. If the threshold has not been reached, re-evaluate your choice of measures or means.

If, after reviewing your choice, you are still unable to eliminate a major risk, or if your tolerance threshold has not been reached, **consider revising this aspect of your project in depth, or removing it**.

Any risk that persists after you have taken steps to reduce or eliminate the risks identified at the outset becomes a **residual risk**. It is possible, and even probable, that privacy risks may persist even after most have been eliminated or minimized. If you accept 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 measure ends up not being chosen, **we recommend that you keep a record of your approach.** Your organization will then remain able to refer to it in the future. It will know why you made certain choices and avoid having to go through the whole process again needlessly.

Review the necessity and proportionality of your project

Once you have completed the risk management process, 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 are proposing to achieve your objectives still seem proportional, given the residual risks? Is all the personal information involved necessary?**

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

If the residual risks are too great, you must consider substantial modifications to your project. This may involve repeating the PIA process in whole or in part, or even reconsidering the project.

4.4 Establish your action plan

Once the privacy factors have been assessed, you should prepare the next stage of the PIA and the project itself by planning the implementation of your chosen measures.

Draft your action plan

Drafting an action plan ensures that the measures and means you have chosen are implemented. Integrating the various actions into your day-to-day activities makes the PIA a reality and ensures that you reap the benefits.

Your action plan should include ways to periodically reassess the effectiveness of the strategies you implement.

Identify those responsible for residual risk management

You should designate individuals responsible for monitoring the evolution of residual risks, otherwise they may be forgotten. These individuals could also be responsible for managing the situation, should it materialize.

Inform the highest authority in your organization

Your organization's highest authorities have a special responsibility for compliance with privacy laws. You should therefore keep them informed of the results of the PIA. They must accept the conclusions of your analysis and endorse the risks that remain despite the means deployed to mitigate them.

Step 1 Step 2 Step 3 Step 4 **Step 5** Step 6

5. Write a report

You should be able to explain and justify your PIA process if required. Preparing a report, even if it is not mandatory, is an excellent way to document your reasoning once the process is completed or when a major milestone has been reached. If you prepare a report, you should update it as your PIA evolves.

This report should be clear and accessible: any reader should be able to understand the nature of the project, how it may affect privacy, and how you have considered, measured, and mitigated the identified risks.

The Commission provides a generic PIA report template (available in French only) **that you may adapt to your needs. The report may also take any other form that adequately reflects your process.**

Prepare your report to document your approach.

5.1 Why write a report?

A PIA report **documents and consolidates** the results of your assessment. In the event of an audit, inspection, or investigation by a regulatory authority, including the Commission, it provides evidence of your actions and thought process. It is also a useful record for your organizational knowledge. If you need to update your PIA or produce a similar one, the report will be a valuable source of information.

A report is the most common and comprehensive option for documenting your process. It can be longer or shorter, depending on the breadth of your PIA (**see section 3.3**). However, it is not mandatory, nor is it the only method available to you. For smaller projects, you could account for the PIA in a number of different ways, for example through minutes or emails attesting to your thought process.

However, please note that the multiplication of supporting documents can be detrimental. Keeping track of your assessment, the evolution of risks, and the implementation of the measures you have selected can be more difficult in the absence of a document that brings together all the relevant information. Similarly, if the Commission needs to verify your PIA, multiple documents can complicate the exercise and work to your disadvantage.

In most cases, you will benefit from opting for a report, especially if you need to certify your PIA to the Commission, for example, as evidence of an agreement to communicate personal information.

5.2 What should the report contain?

Your report should first present the essentials of your project, its context, and your analysis. It should also mention that your report has been approved by the highest authorities in your organization.

Finally, your report should include additional information in the form of appendices, if applicable:

- A list of your relevant privacy and information management policies;
- A summary of security notices produced in collaboration with providers or partners (such as intrusion tests);
- A communication agreement signed after the PIA;
- Certifications obtained as part of your project (when an evaluation body certifies that your product or service complies with certain requirements), etc.

The following table provides an overview of the elements that could be included in your report, with appropriate references to the sections of this guide and to the generic report template proposed by the Commission (available in French only).

Elements	Section of the guide	Section of the generic report template
The legal context that motivated the PIA, if applicable	Section 1.1	Summary of the assessment
A description of your project, what motivated it (context), and the objectives pursued	Section 2.1 Section 2.2	Section 1: Description of the project and the objective of the PIA
All the parties involved in the project, including a description of their roles and responsibilities	Section 2.3	Summary of the assessment Section 2. Roles and responsibilities
A summary of consultations, if any	Section 2.3	Section 2. Roles and responsibilities
An overview of the inventory of personal information involved (categories, purposes, quantity, etc.)	Section 3.1	Section 3. Personal information involved and scope of assessment
An overview of the mapping of personal information involved (sources, mediums, recipients, systems used, persons with access, etc.)	Section 3.2	
An assessment of the criteria for sensitivity, purpose, quantity, distribution, and medium of personal information, and a justification of the breadth of the PIA	Section 3.3	
A description of the means implemented to comply with personal information protection obligations and principles (including sectoral or situational, as required)	Section 3.4 Section 4.1	Section 4. Compliance with obligations and principles respecting the protection of personal information
Proof of compliance with the specific criteria associated with the legal situation prompting the PIA, if applicable	Section 7	
A list and categorization of identified risks to persons concerned	Section 4.2	Section 5: Identification of risks and mitigation strategies
The strategies, mechanisms and measures deployed to eliminate or reduce these risks	Section 4.3	
The persons responsible for implementing these strategies, mechanisms and measures	Section 4.4	Section 6. Action plan
An action plan with a schedule, including a periodic reassessment of the measures implemented	Section 4.4	
Report approval by the organization's highest authorities (including names, titles, signatures, date, etc.)	Section 4.4	Section 7. Report approval and versions
Any relevant documents	N/A	Attached documents

5.3 Should the report be circulated?

As a best practice to ensure transparency, your organization may decide to publish a condensed version of the PIA report on its website, or by other means. This may reflect a commitment to comply with the law and to keep the persons concerned informed.

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

5.4 Should the report be sent to the Commission?

You are expected to submit a PIA report to the Commission prior to signing an agreement (**see section 7.3**, **section 7.4**, **section 7.5**). A written document attesting to the PIA process demonstrates that your organization has met its obligation. It provides a clear understanding of how each criterion was analyzed, and which elements were considered.

In other cases, it is not necessary to proactively submit a PIA report to the Commission. However, the Commission may request to see the report as part of its monitoring activities.

6. Maintain the assessment up to date

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

To ensure that your measures are effective, you must monitor their application and revise them in light of emerging risks, or changes to your project: the development of a new line of business, plans to implement a complementary service to the existing transactional system, etc.

Active measurement control tools, such as a security dashboard, will allow you to monitor the consistent and integrated application of the strategies and measures in place.

Step 7

7. Particularities in certain situations

The general PIA process is always the same. However, you will need to take certain particularities into account depending on the legal situation that prompts your assessment.

This section provides details on certain concepts included in the law, on the conclusion of agreements, and on the evaluation of specific criteria in certain situations.

Include in your report:

- **A demonstration that the specific criteria the PIA must address have been met, where applicable.**

7.1 Transfer of personal information outside of Québec

These precisions concern the situation covered by 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 from outside Québec** with the task of collecting, using, communicating, or retaining such information on your behalf.

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

- The sensitivity of the information to be communicated;
- The purpose for which it is to be used;
- The security measures, including contractual ones, it would benefit from;
- The legal framework applicable in the state where the information would be communicated, including the personal information protection principles applicable in that state.

You may communicate the information if the PIA establishes that it would receive **adequate protection**, in particular in accordance with **generally recognized principles** regarding the protection of personal information.

What are "generally recognized principles"?

The Access Act and the Private Sector Act do not define "generally recognized principles."

However, it can be assumed that they are general rules designed to ensure the protection of personal information, and respect for the rights and interests of the persons concerned.

Without being exhaustive or definitive, the following is a list of principles embodied in numerous privacy laws and other significant privacy documents, such as standards or guidelines:[18]

- **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, notably by designating a person responsible. They document their compliance and decisions regarding the protection of personal information.

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

- **Identifying purposes**. The purposes for which personal information is collected are identified prior to collection.
- **Limiting collection**. Organizations collect only the information necessary for the purposes identified. Information is collected by fair and lawful means. Invasion of privacy is minimized.
- **Consent**. Persons concerned are adequately informed of the identified purposes and freely consent to them unless an exception applies.
- **Privacy by design and default**. Products/services are designed to respect the privacy of the persons concerned. If they include privacy settings, these protect privacy by default.
- **Limiting use, communication, and retention**. Organizations use and communicate personal information collected for identified purposes, or compatible purposes, unless consent is provided, or in the case of legal exceptions. Access to personal information is limited to authorized persons, and personal information is retained only as long as 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**. At all times, organizations take appropriate security measures to protect the information they hold against loss, theft, or unauthorized modification, communication, or destruction. These measures are appropriate for both the sensitivity of the information and 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 persons concerned at the time of collection or consent. They provide the public with their contact details as well as clear information on their policies and practices for managing personal information.
- **Individual rights.** Persons concerned can access their personal information and request rectification or, in certain cases, deletion. Organizations set up accessible processes to enable these rights to be exercised.
- **Remedies**. In the event of dissatisfaction, individuals can contest a refusal for them to exercise a right, or lodge a complaint with the organization or a competent body.

What is “adequate protection”?

Again in this case, the Access Act and the Private Sector Act do not define “adequate protection.”

We can think of it as protection that offers **legal** (legislation of the state of destination) and **contractual** (agreement with the receiving organization) guarantees that meet all generally recognized protection principles, and are appropriate to the sensitivity and purpose of the information concerned.

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 be included in the written agreement following a PIA?

The communication of personal information outside of Québec must be covered by a written agreement between the third party and you. This agreement must take into account, in particular, the results of the PIA. If necessary, it must include agreed-upon terms and conditions to mitigate the risks identified in the PIA in order to achieve adequate protection.

7.2 Information or electronic service delivery system

These precisions concern the situation covered by sections 63.5 of the Access Act and 3.3 of the Private Sector Act.

A PIA is required for any project related to an **information or electronic service delivery system** involving the collection, use, communication, retention, or destruction of personal information. Such projects may involve:

- Acquisition;
- Development;
- Overhaul.

What is an information or electronic service delivery system?

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

- Computerized file-processing system;
- Videoconferencing or collaboration software;
- Biometric systems;
- Artificial intelligence system;
- Smart card/RFID system;
- Video surveillance system;
- Statistical systems;
- Payroll system.

An **electronic service delivery system** can take the form of:

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

7.3 Communication for study or research, or for the production of statistics

These precisions concern the situation covered by 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 persons concerned to a person or body wishing to use the information for **study or research purposes, or for the production of statistics** (hereafter "research"), is permitted if a PIA concludes that certain criteria are met.

Who must carry out the assessment: the organization or the researcher?

The PIA should be carried out by the **organization holding/controlling** the personal information, based notably on the information provided by the person or body. Indeed, the person or body is in a good position, for instance, to describe how the personal information will be used once it has been communicated, why it is necessary for the research, and what security measures are in place.

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.

What must the PIA demonstrate?

The PIA can be carried out by following the general approach presented in this guide. However, the PIA should allow you to justify your conclusion regarding compliance with each of the five criteria set out in the law.

1. **The objective can be achieved only if the information is communicated in a form allowing the persons concerned to be identified**

For example, if it is possible to carry out the research or study using **anonymized information**[19] or synthetic data, the communication of personal information is not authorized.

If the research can be carried out using **de-identified information**,[20] only this information should be communicated. It is important to note that this information is still confidential personal information. It is up to the person or body to convince you of the need to use personal information, de-identified or not. The use of non-de-identified information requires a compelling explanation that the research cannot be carried out without the "direct identifiers."

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

As an exception to the consent requirement, the organization must be able to conclude that it is unreasonable to require the consent of all persons whose information is required for the purposes of the research. 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 individuals whose contact details are not up to date;
- The research could involve information from individuals who are either incapable of consenting or deceased;
- The research may rely on de-identified information held by your organization, making it impossible for the research person or body to obtain consent;
- In certain cases, creating a representative sample may require that you avoid introducing a bias by using only data from individuals willing to consent.

Beware! Lack of human, financial, or material resources is not a sufficient reason to demonstrate that obtaining consent is unreasonable.

[19] Information is **anonymized** when it is reasonably foreseeable under 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 as well as the criteria and procedures determined by regulation.
[20] Information is **de-identified** when it prevents direct identification of the person concerned.

3. The objective pursued outweighs, with respect to the public interest, the impact of communicating and using the information on the privacy of the persons concerned

The purpose of this part of the PIA is to weigh the public interest objective of the research against the consequences of the communication and use of personal information on the privacy of the persons concerned.

This analysis must first identify and describe the various elements and factors to be considered in carrying out this balancing.

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 some examples of questions to ask yourself when assessing a person or body's request:

- What is the purpose of the research and why is it in the public interest?
- What benefits are expected for society?
- What are the various consequences for the privacy of the persons concerned by the communication of information?
- Can these consequences be minimized as part of the 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 persons concerned? Will these practices affect the risk of communication of personal information about one or more persons?
- What makes it possible to believe that the public interest outweighs the impact of the communication and use of personal information on the privacy of the persons concerned?

Beware! The assessment of this criterion is not limited to setting out the purpose of the research, nor simply stating a general effect, such as the fact that it will increase knowledge in a field of activity. **The expected benefits of the research in relation to public interest must be specified and weighed against the consequences for the privacy of the individuals whose information will be used for the purposes of the research.**

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

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

5. Only the necessary information is communicated

The PIA must indicate how the organization will ensure that only the **necessary** information for the research will be communicated. Particular attention should be paid to "direct and indirect identifiers" (related to the first criterion; for example, addresses, complete postal codes, health insurance numbers, dates of birth, or ages) and to particularly sensitive information.

What are the steps following a 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 send it to the Commission. The agreement is in force 30 days after it is received by the Commission.

Should a PIA report be sent to the Commission?

Yes, a PIA report must be sent with the agreement to the Commission. A written document attesting to the PIA process allows your organization to demonstrate that it has met its obligation. It explains how each criterion was analyzed and which elements were considered.

7.4 Collection by a public body on behalf of another public body

These precisions concern the situation covered by section 64 of the Access Act.

A PIA is required when a public body:

- Collects personal information necessary for carrying out the functions or implementing a program of another public body with which it collaborates;
- Collects this type of information for the delivery of services or the achievement of a shared mission;
  - For example, a public body may collect personal information to verify individuals' eligibility for a program it administers.

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

Who must carry out the assessment?

It is the public body that will ultimately hold the personal information, meaning the one asking another public body to collect personal information on its behalf, which should conduct the PIA, collaborating as needed with the public body assisting it. The latter is well placed, for example, to describe how personal information will be collected, under what security measures, etc.

What are the steps following a PIA?

Collaborating organizations must enter into a written agreement, the content of which is specified in section 64 of the Access Act. They must then send it to the Commission. The agreement comes into force 30 days after it is received by the Commission.

Should a PIA report be sent to the Commission?

Yes, a PIA report must be sent with the agreement to the Commission. A written document attesting to the PIA process demonstrates that your organization has met its obligation.

[21] 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.

7.5 Other communication without consent (public sector)

These precisions concern the situation covered by section 68 of the Access Act.

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

- To another public body, in Québec or elsewhere:
  - For the exercise of its functions or the implementation of a program it manages;
  - When the communication is clearly for the benefit of the individual concerned;
- To any person or public body:
  - Where exceptional circumstances justify doing so;
  - For the provision, by a public body, of a service to be rendered to the individual concerned, notably for identification purposes.

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

Who must carry out the assessment?

The PIA should be carried out by **the organization holding the personal information**, in collaboration with the recipient of the communication if necessary. 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 a PIA?

For these other types of communication to be carried out, the PIA must allow you to conclude that the following four criteria have been met:

1. **The purpose can be achieved only if the information is communicated in a form allowing the persons concerned to be identified**

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.

[22] 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.

If the purpose of the communication can be achieved using **de-identified information**, only such 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 de-identified or not.

The use of non-de-identified information requires a convincing demonstration of the impossibility of carrying out the communication without "direct identifiers."

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

Since this is a consent exception, you must be able to conclude that it is unreasonable to require the consent of all persons whose information is required for the purposes of the contemplated communication.

Beware! Lack of human, financial, or material resources is not a sufficient reason to demonstrate that obtaining consent is unreasonable.

3. The objective outweighs, with regards to the public interest, the impact of communicating and using the information on the privacy of the persons concerned

The purpose of this part of the PIA is to weigh the objective of the communication with regards to the public interest against the impacts of the communication and use of personal information on the privacy of the persons concerned.

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

You must then determine whether the public interest purpose of communication outweighs the potential impact on the privacy of the persons concerned.

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

- What is the purpose of the communication, and why is it in the public interest?
- What benefits are expected for the persons concerned and for society as a whole?
- What are the various consequences on the privacy of the persons concerned by the communication of information?
- Can these consequences be minimized within the framework of the communication? 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 persons concerned? Will these practices influence the risk of communication of personal information about one or more persons?
- 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 persons concerned?

Beware! The assessment of this criterion is not limited to setting out the purpose of the communication, or to simply stating a general effect, such as "improved services." **The expected benefits of the proposed communication in relation to the public interest must be specified and weighed against the consequences for the privacy of the persons concerned whose information will be communicated**.

4. Personal information is used in a way that ensures confidentiality

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

What are the steps following a 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 send it to the Commission. The agreement comes into force 30 days after it is received by the Commission.

Should a PIA report be sent to the Commission?

Yes, a PIA report must be sent with the agreement to the Commission. A written document attesting to the PIA process demonstrates that your organization has met its obligation. It explains how each criterion was analyzed, and which elements were considered.

Was this tool helpful?
Fill out [the CAI's] short satisfaction survey (available in French only)!

Commision d'accès à l'information du Québec

Montréal
2045, Stanley Street
Office 900
Montréal (Québec) H3A 2V4
Phone : 514 873-4196

Québec
525, boul. René-Lévesque Est
Office 2.36
Québec (Québec) G1R 5S9
Phone : 418 528-7741

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