Commission d’accès à l’information

Biometrics: Compliance principles and legal obligations of organizations

Practical guide for public bodies and private enterprises

September 2022

Unofficial translation by BLG LLP

Source: Biométrie : principes à respecter et obligations légales des organisations — Guide d’accompagnement pour les organismes publics et les entreprises, CAI

Version 2.0

This guide was first published in July 2020. This new version reflects the enactment of *An Act to modernize legislative provisions as regards the protection of personal information* (SQ 2021, c. 25). It incorporates the relevant changes coming into force in September 2022.

INTRODUCTION

The *Commission d'accès à l'information* (the Commission) promotes and enforces citizens' rights regarding access to documents of public bodies, as well as the protection of their personal information held by public bodies and private enterprises.

For several years, the Commission has noted an **increased use of biometrics** in both the private and public sectors. This technology, which has become increasingly accessible due to technological advances (algorithms, machine learning, storage capabilities), has become affordable in terms of both installation and maintenance. **Biometric systems** are seen as a simple and convenient way of achieving several purposes (control of employee schedules, identity verification, access to premises, etc.). Some companies even offer **turnkey versions of such systems,** making them easier to adopt.

However, the popularity of biometrics has led to **a certain trivialization** of its privacy implications. While it is said to be safe, we often forget that its use poses **risks to individuals' privacy.** The legal framework that applies to biometrics is also not well known.

It is in this context that this guide has been developed, whose objectives and target audience are presented in the following pages.

WHAT ARE THE OBJECTIVES OF THIS GUIDE?

The Commission is publishing this guide to:

> Raise awareness among public bodies and private-sector organizations of **their responsibilities and obligations** in protecting personal information when using biometrics;

> Assist them in completing **the declaration that they must submit to the Commission,** before starting to use biometrics, in either of the following two cases:

- If they require the use of a biometric system, or a process for capturing biometric characteristics or measurements, to verify or confirm the identity of one or more individuals;

- If they create a database of biometric characteristics or measurements – in this case, the disclosure must be made **at least 60 days** before the database is operational.

The Commission provides a declaration form (available in French only) to that effect. This form allows you to provide all the required information.

WHO IS THIS GUIDE FOR?

This guide **is aimed at both public bodies and private enterprises of all sizes.** It is intended for:

- Decision-makers;
- Those responsible for implementing projects that involve the use of biometrics;
- Privacy officers.

Legal obligations with regard to biometrics in Québec apply to **any organization wishing to use a biometric system or a process to capture biometric characteristics or measurements.**

This guide **also applies to private enterprises that provide such solutions.** It is important that they know these rules in order to properly advise their clients, to avoid misleading them, and to offer products that comply with the legislation applicable in Québec.

WHAT ARE BIOMETRICS?

Throughout this guide, **biometrics** refers to the set of techniques that analyze one or more unique characteristics of a person (physical, behavioural, or biological) in order to determine or prove their identity. The digitalization of biometrics allows for the automation of this identification or authentication. For the most part, biometrics are mainly used today through automated systems.

Some projects or technologies may use morphological, behavioural, or biological characteristics **for purposes other than verifying or confirming the identity of individuals:** thermal cameras, anonymous video analysis (AVA), connected health bracelets, emotion recognition systems, etc. Although these uses are not specifically covered by all the principles contained in this guide, either the *Act respecting Access to documents held by public bodies and the Protection of personal information* (Access Act) or the *Act respecting the protection of personal information in the private sector* (Private Sector Act) applies to organizations implementing such projects.

No matter the project, if biometric characteristics or measurements are involved, it is recommended to conduct a privacy impact assessment (see the introduction to Section 1) as this is sensitive personal information (see below).

Note that as of September 22, 2023, a privacy impact assessment will be required for any project involving the acquisition, development, or overhaul of an information system or electronic service delivery system that involves the collection, use, communication, keeping, or destruction of personal information. The Commission is already offering a guide for this process.

Biometrics categories

There are three broad categories of biometrics:

- **Morphological biometrics** is based on the identification of specific physical traits. It includes, but is not limited to, the recognition of fingerprints, the shape of the hand, the face,[1] the retina, and the iris;

[1] The Commission and some of its counterparts in Canada released a privacy guidance document in 2022 for police services' use of facial recognition. This document contains potentially interesting elements for any organization wishing to deploy this technology.

- **Behavioural biometrics** is based on the analysis of certain behaviours of a person, such as the tracing of their signature, their voiceprint, their gait, the way they type on a keyboard, etc.

- **Biological biometrics** is based on an analysis of the biological traces of a person, such as DNA, blood, saliva, urine, odours, etc.

The **biometric characteristics or measurements** derived from these analyses are also referred to as **biometric information** through this guide. Their format can be either raw (image or print) or coded (code or encrypted template extracted from an image or a print).

Whether or not they are compiled or stored in **databases of biometric characteristics or measurements,** biometric information is subject to a specific legal framework when it is used to verify or confirm an individual's identity.

Identification and authentication

The principles listed in this guide apply to any biometrics project that serves one of the following two purposes:

- **Identification,** which consists of finding an identity in a database among several other identities. The biometric characteristics or measurements of a person whose identity is not known are compared with those contained in the database. The objective is to answer the question, *"Who is this person?"*

- **Authentication,** which consists in validating an identity by making a "one-to-one" comparison with biometric characteristics or measurements associated with a known person. The objective is to answer the question, *"Is this person who they claim to be?"*

Any technology that relies on biometrics for identification or authentication is called a biometric system. More generally, this guide also covers any method that enables the capture of biometric characteristics or measurements. The Commission therefore uses the term **"biometric system or process"** throughout the document.

Such technology typically presents two phases:

- **Enrollment or registration,** where biometric characteristics or measurements are captured for the first time and recorded;

- **Recognition,** during which the above identification or authentication processes take place.

Biometric characteristics and measurements: Personal information

Biometric information is **personal information,** that is, information that relates to an individual and allows them to be identified.[2] It is unique, distinctive, and persistent over time.

This is the case for images (of the face, iris, etc.) and prints (fingers, hand outline, voice, keystroke patterns, etc.), whether they are static (fixed images or prints) or dynamic (animated images or prints, or those with a temporal dimension).

This is also true of **any code (also called a template or model), digital or otherwise, that is derived from these images using an algorithm.** To the extent that this code, which constitutes a characteristic or a biometric measurement, is retained for the subsequent recognition of the person, **it makes it possible to identify them,** being distinctive by nature.

Biometric characteristics and measurements: Sensitive information

Biometric information is particularly **sensitive**.[3] It represents **permanent and distinctive** characteristics: **unique** identifiers composed of **intimate** information.

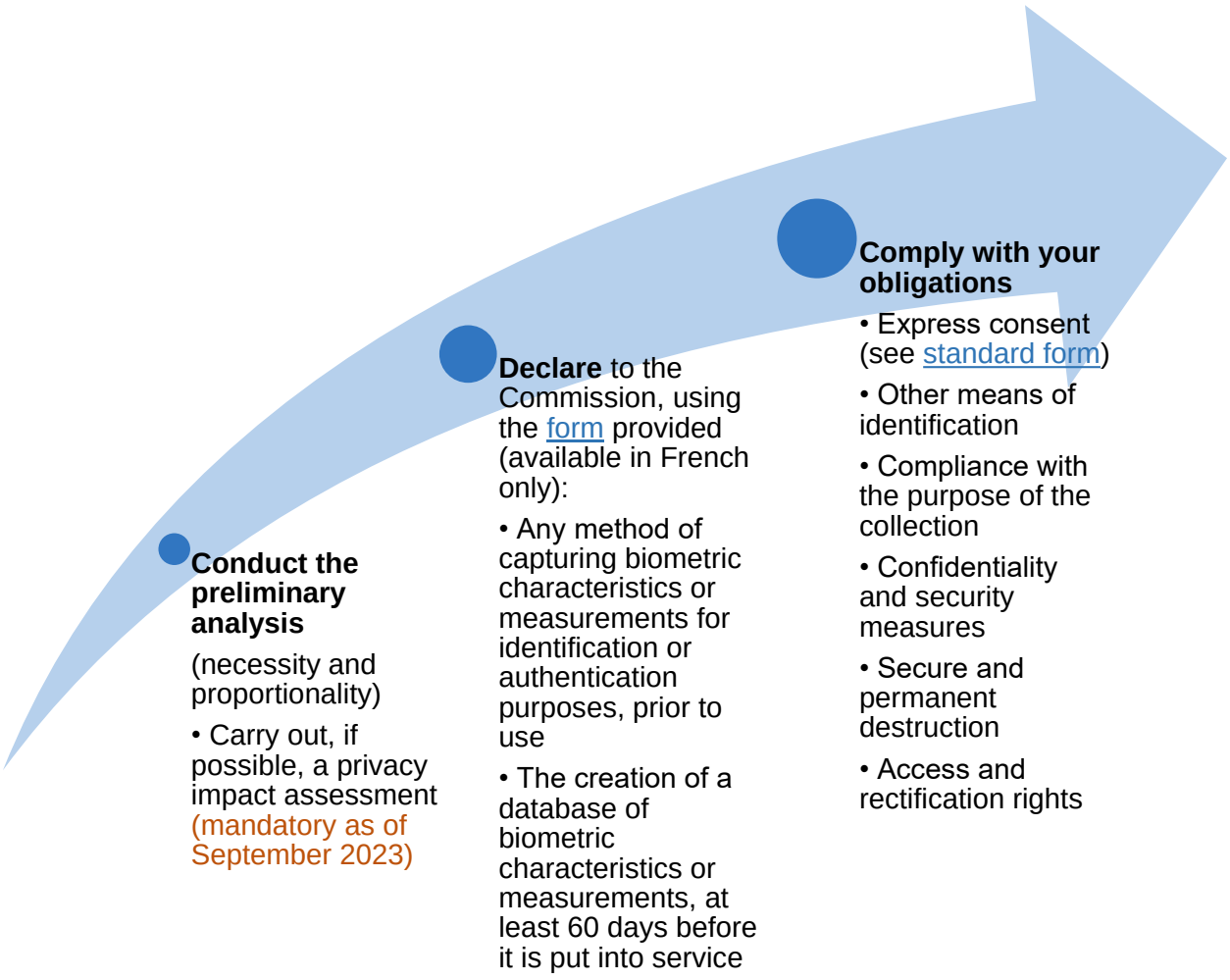
Similarly, some of this information can be **deduced from information other** than an individual's identity. For example, iris scanning and gait analysis can uncover a disease or disability. Biometric measurements or characteristics can also reveal ethnic origins.

Finally, if the confidentiality of this information is compromised, there **may be serious consequences** for the person concerned: while it is possible to replace a magnetic card, a personal identification number (PIN), or a password, it is not possible to change one's face or fingerprints.

2 Access Act, section 54; Private Sector Act, section 2.

3 Effective September 22, 2023, amendments to sections 59 of the Access Act and 12 of the Privacy Act will explicitly state that biometric information is sensitive.

SUMMARY OF THE PROCESS



Contact the Commission if you have any questions about this guide or the declaration to be submitted. Please note, however, that we do not provide legal opinions or specific advice, nor do we offer certification.

QUÉBEC
Office 2.36
525 René-Lévesque Boulevard East
Québec City, Québec G1R 5S9
Telephone: (418) 528-7741
Fax: (418) 529-3102

MONTRÉAL
Office 900
2045 Stanley Street
Montréal, Québec H3A 2V4
Telephone: (514) 873-4196
Fax: (514) 844-6170

Toll-Free
1-888-528-7741

Email
renseignements@cai.gouv.qc.ca

Website
www.cai.gouv.qc.ca

TABLE OF CONTENTS

1. CONDUCT THE PRELIMINARY ANALYSIS

The use of biometrics by a public body or private enterprise involves **collecting, using, retaining, communicating, or destroying particularly sensitive personal information.**

You must make a **careful assessment** before implementing a biometric system or process. To do so, you need to know the applicable rules, and take into account the sensitive nature of personal biometric information when assessing both the lawfulness of such a project and the obligations to be respected when deploying the chosen solution, if applicable.

The best way to do this is to **conduct a Privacy Impact Assessment**[4]. The Commission has published a guide to help with this process. Consult it to guide your analysis.

1.1. Comply with applicable legislation

The collection and use of biometric information by a public organization or a private enterprise is governed by **several laws** in Québec. The Commission is the body responsible for enforcing the provisions applicable to the use of biometrics contained in the following three acts:

- *Act to establish a legal framework for information technology*;[5]
- *Act respecting Access to documents held by public bodies and the Protection of personal information*;[6]
- *An Act respecting the protection of personal information in the private sector*.[7]

The Commission can exercise different powers under these acts. For example, it can conduct an inspection or an investigation. With regard to databases of biometric characteristics or measurements specifically, it may, inter alia:

- **Issue any order** regarding a database to determine its creation, use, consultation, communication, and retention, including the archiving or destruction of the characteristics or measures taken to identify individuals;

4 **As of September 22, 2023, a privacy impact assessment will be mandatory for any project to acquire, develop, or overhaul an information system or electronic service delivery system involving the collection, use, communication, keeping, or destruction of personal information.**

5 CQLR, c. C-1-1, hereinafter the IT Act.

6 CQLR, c. A-2.1, hereinafter the Access Act.

7 CQLR, c. P-39.1, hereinafter the Private Sector Act.

- **Suspend or prohibit** the implementation of a database;
- Ultimately **order the destruction** of a database if it does not comply with an order of the Commission, or if it otherwise infringes on privacy.

Therefore, before deciding to implement a biometric system or process within your organization and commit time and resources to this project, make sure it complies with **all applicable legislation.**

1.2. Collect only the necessary information

Both the Private Sector Act and the Access Act provide that only **necessary** personal information may be collected.[8] **This rule cannot be waived by obtaining consent from the person concerned.**

Therefore, you **must consider whether it is necessary** to collect personal information, including biometric measurements or characteristics.[9]

The necessity of collecting biometric information is assessed against the following criteria.

1.2.1. The purpose of the collection must be important, legitimate and real

Your use of biometrics must be aimed at **solving a problematic situation,** thus pursuing an **important and legitimate** purpose.

You cannot simply indicate the purpose of the biometric system or process (for instance, "verification of employee identity and hours worked," "client identity confirmation"): you must **specify and document** the problem encountered in pursuing this purpose, which justifies the collection of personal information using biometrics.

Examples of problematic situations to document when assessing the necessity of collection:

- Fraud and time theft;
- Work environment and context that make it very difficult to monitor a person's arrival and departure times, or their presence at work;
- Need for increased access control to highly secure locations.

8 Access Act, section 64, Private Sector Act, sections 5 and 6.

9 This analysis is part of the privacy impact assessment process.

✓ ***Ask yourself the following questions:***

> **Why** is this information collected?

> What is **the purpose** of using biometrics?

> Is this a **real and concrete problem**?

✓ ***You must be able to:***

> **Identify the problem** or situation you want to correct. Usefulness or convenience ("it's simpler, more practical") does not justify the collection of biometric characteristics or measurements.

> **Document the scope of the problem** or situation. This problem must be significant and real rather than possible or potential. It must justify the legitimacy of collecting such sensitive information. You must therefore identify the concrete evidence of its existence, or the likelihood of occurrence and its significance.

1.2.2. The collection must be proportional to the purpose pursued

The use of biometrics must be **a solution proportional** to the purpose pursued, and take into account the other means at your disposal and the consequences for the persons concerned. You must consider the sensitive nature of biometric information in your assessment. Its collection constitutes a high degree of intrusion into the privacy of individuals.

You must analyze the proportionality of your use of biometrics in relation to the purpose pursued in three stages:

✓ ***Does the collection of biometric information achieve the purpose that motivates the implementation of your biometric system or process? Is it an effective (rational) and proven means of achieving this purpose?***

> Ensure that the biometric system or process is **an adequate solution** to the identified problem. Document the effectiveness of this solution in resolving the situation.

> Consider **the limitations** of the proposed solution. For example, some biometric systems have error rates that could compromise the effectiveness of this tool in achieving your goal.

✓ ***Is there a less intrusive way to achieve the purpose of this biometric system or process? Can you minimize the invasion of privacy that the use of biometrics in your project represents?***

> Explore **other means** at your disposal to achieve the desired purpose, to solve the problematic situation for which you want to use biometrics.

> Identify those that **are less invasive of the privacy** of the persons concerned, including those that do not involve biometrics or that minimize the collection of personal information by your organization.

> How do these other means **not achieve the purpose** pursued or solve the problem identified? Why would biometrics be required if these other solutions are available to you? If you have tested other solutions that have proven ineffective in achieving the purpose, document this situation and, more importantly, **explain why these other solutions were not effective or adequate.**

> If there is no other reasonably effective way to achieve the purpose that is less intrusive on the privacy of individuals, identify **ways to minimize the invasion of privacy** that your project represents. What measures can you implement to reduce privacy risks?

Examples of existing risk mitigation measures include:

> Collect only the code extracted by the algorithm from a fingerprint rather than the raw image;

> Use a decentralized storage system;

> Implement strict confidentiality measures.

✓ ***Are the benefits of biometrics greater than the invasion of privacy of the individuals involved and the potential consequences of implementing the biometric system or process?***

> **Document the benefits** of biometrics to achieve the intended purpose.

> **Document the disadvantages** and risks of violations to privacy or personal information protection for the persons concerned, as well as other potential consequences. Consider all the concrete consequences that could occur.

Examples of consequences:

- Violation of other rights;
- Consequences in the event of a confidentiality incident involving biometric information (such as identity theft).

- **Weigh the pros and cons** of the biometric system or process.

1.3. Following your analysis...

If your assessment **does not allow you to conclude on the necessity** and proportionality of collecting biometric information...

- **Your project does not comply with applicable legislation.** Assess the possibility of modifying your project to bring it to compliance for the purpose of filing a declaration with the Commission. Otherwise, you should consider an alternative solution.

If you **conclude that it is necessary** to collect biometric characteristics or measurements...

- **You can collect only those that are essential for identity verification or confirmation.**
- The law provides that the identity of a person can only be established by using **the minimum number** of characteristics or measurements necessary to link them to the action they are taking.[10] For example, if you can identify a person with a single fingerprint, you should not collect all ten fingerprints.
- You must **declare** your **biometric** system or process to the Commission prior to its use; in the event of a biometric measurement database being created, the declaration to the Commission must be made at least 60 days before it is put into service.

In order to continue the process, you must comply with a number of obligations, which are outlined below.

[10] IT Act, section 44.

2. KNOW AND COMPLY WITH YOUR OBLIGATIONS

2.1. *Before* using the biometric system or process

2.1.1. Declare the biometric system or process to the Commission

Before using your biometric system or process, you must **declare it to the Commission,** which makes available a form to provide all the required information.

✓ ***Timing of the declaration***

You must submit your declaration **before** your biometric system or process is **put into service.**[11] More specifically, in the case of the creation of a database of biometric characteristics or measurements, you must send it to the Commission **at least 60 days before the database is put into service**.[12]

✓ ***Processing by the Commission***

Once your declaration has been submitted to the Commission, it will send you an acknowledgement of receipt, reminding you of your obligations under certain aspects of the law. **This acknowledgement does not mean that the Commission *approves* or *authorizes* your biometrics project in whole or in part.**

If the declaration is incomplete or raises certain questions, the Commission may ask you to provide additional information.

Based on the information received, the Commission may decide, depending on the type of declaration:

- not to take action;
- to send a letter highlighting problematic elements;
- to exercise the supervisory powers mentioned on pages 1 and 2.

At all times, your organization remains responsible for meeting the obligations set out in the law. Even after the database, system, or biometric process has been implemented, the Commission may initiate an inspection or investigation under the Access Act or the Private Sector Act if it deems it necessary.

[11] IT Act, sections 44 and 45.

[12] IT Act, section 45.

2.2. *When* using a biometric system or process

This section provides an overview of your obligations when using a biometric system or process. For a general overview of your privacy responsibilities, visit the CAI's French-only website (section for public bodies; section for businesses).

2.2.1. Obtain express consent of the persons concerned and provide for an alternative means of identification in the event of refusal

The law prohibits **requiring** that the verification or confirmation of a person's identity be carried out by a process that captures biometric characteristics or measurements.[13] This implies that:

- You must obtain **the valid and express consent** of each individual;
- You must **provide an alternative solution** to verify or confirm identity, in the event of refusal or withdrawal of consent;
- You may not use biometric characteristics or measurements **without the knowledge** of the person concerned (captured without their knowledge).

✓ ***Express consent***

Consent is considered "express" when it is given **explicitly and unequivocally.** As such, a person must make a positive gesture clearly indicating their agreement. This is generally contrasted with implied or tacit consent, which is derived from behaviour, conduct, or gestures.

The best way to convey consent in an explicit way is **to sign a document.** It will also allow you to report on compliance if necessary.

Obtaining consent **does not relieve you of your obligation** to collect only the necessary personal information (see detailed analysis in section 1.2).

✓ ***Free, informed, specific, and time-limited consent***

In order for consent to be legally valid under the applicable principles in privacy laws,[14] it must be:

[13] IT Act, section 44.

[14] Private Sector Act, section 14. These criteria are also applied in the public sector; as of **September 22, 2023, they will be explicitly included in section 53.1 of the Access Act as well.**

- **Free:** no undue coercion or pressure (for example, a threat, a financial or other type of incentive, etc.) should influence the person's decision. They may withdraw their consent at any time

- **Informed:** the data subject must have sufficient information to understand what they are consenting to. You must therefore give them **all** the relevant information:[15]

    - the purpose of the biometric system or process;
    - the biometric characteristics or measurements that will be collected;
    - the procedure used for collecting biometric characteristics or measurements;
    - other personal information that will be collected and associated with it;
    - the intended use of biometrics and personal information;
    - the categories of persons who will have access to it within the organization;
    - the security measures put in place to protect them (such as encryption, storage location, de-identification, etc.);
    - the parameters governing their possible communication;
    - their retention period;
    - how to exercise the right of access and rectification;
    - the possibility for the person to refuse to provide biometric characteristics or measurements and use another means of identification.

You must present this information in a **clear and understandable** manner, using **specific but accessible terms** that allow all persons concerned to understand the scope and consequences of their consent. Avoid complex legal language.[16]

- **Specific:** the **scope** of consent must be **clearly defined** and linked to the purposes pursued by the biometric system or process. Avoid asking for broad or vague consent using phrases such as "any information deemed necessary."

- **Limited in time:** consent is given for **a defined period,** which is specified either by duration (for example, a number of months) or by an event or situation (such as termination of employment). Avoid asking for extended consent using phrases like "as long as necessary."

[15] See, for example, the Access Act, section 65; the Private Sector Act, section 8.

[16] In this regard, note that **as of September 22, 2023, you will be required to provide this information in simple and clear language.**

Regardless of how you obtain consent, **be thorough** in presenting the information to the individuals concerned and **devote the necessary time** to this crucial step in the process.

An example of a consent form (available in French only) is available on the Commission's website. This **must be adapted** to the particularities of the biometric system or process considered by your organization.

✓ ***Authentication upon enrollment / registration***

If the person consents to the collection of their biometric information, you will certainly have to confirm their identity before their initial registration. The most common way of doing this is through the use of identification documents. In this respect, the Commission invites you to consult its information sheet for businesses (available in French only), which contains important details on the best practices to be developed using identity documents — in general, these also apply to public bodies. In summary, **it is possible to ask to see an ID, but not to collect its contents** in any way.

If you collect other personal information at the time of enrollment or registration, ensure that collection is necessary (see section 1.2) and comply with your usual legal obligations regarding the protection of personal information.

✓ ***Means of identification in case of refusal***

The requirement to obtain express consent before you can identify a person using biometric characteristics or measures means that you cannot impose this method. The individuals concerned **should not be pressured or inconvenienced** in relation to their choice. You must provide an alternative solution for those who refuse to consent or withdraw their consent.

Examples of alternative solutions:

> Access card system;

> Use of unique tokens;

> Use of a password or identification code.

✓ ***No collection of biometric information without the knowledge of the individual***

The law prohibits the identification of a person or the verification of their identity using biometric characteristics or measurements **without their knowledge**.[17] This obligation is similar to that of obtaining express consent. This implies that you are to collect biometric characteristics and measurements **directly from the person concerned.**

[17] IT Act, section 44.

2.2.2. Respect the purpose of the collection

The biometric information you collect must be used **exclusively** to achieve the original purpose of the biometric system or process,[18] unless the person concerned has given their **express** consent or an exception is provided by law. Moreover, any other information about a person that could be discovered by way of biometric characteristics or measurements cannot be used to make a decision about that person.[19]

2.2.3. Implement confidentiality and security measures

Remember: biometric information is sensitive personal information because it is permanent, unique, distinctive, and intimate. It may be coveted by malicious actors. Therefore, it must be protected by **strong confidentiality and security measures,** which take into account, in particular, its quantity, distribution, and medium.[20]

You must take into account the context in which the biometric system or process for which you are responsible is implemented when establishing these measures. **Physical, IT, logical, and organizational security must be provided in a number of ways**.[21]

To ensure the secure storage and confidentiality of biometric information, your measures should include data format, storage medium, server location, privacy-enhancing technologies, and restricting access and communication involving third parties.

✓ ***Data format***

You should **favour systems that irreversibly convert** an image or print **into code:** these limit the sensitivity of the biometric characteristics and measurements collected and stored. Once an algorithm has performed the conversion, it should be impossible to reconstruct the original image or print.

This not only prevents their reuse for new analyses unrelated to the purposes for which they were collected, it also guarantees persons concerned that in the event of data loss or theft, their biometric identifiers may not be used directly to impersonate them in another biometric system.

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

[19] IT Act, section 44, para. 2.

[20] IT Act, sections 40 and 41; Access Act, sections 53, 62 and 63.1; Private Sector Act, sections 10 and 20.

[21] The Privacy Impact Assessment process also involves assessing these aspects of security and to provide for appropriate measures, taking into account the context.

✓ ***Storage medium***

The storage of biometric information can be **centralized** in a single database. All the data is then collected, which can have very significant effects in the event of a confidentiality incident (unauthorized access, data leak, etc.).[22]

Where possible, you should opt for a **decentralized** solution to mitigate this risk. Using an external medium, either individual or portable, for the storage of biometric characteristics or measurements that have been coded or securely encrypted, under the control of the person concerned, would be an example of a decentralized solution.

✓ ***Server location***

If you absolutely have to create a database that centralizes the information, it should be kept **locally on a secure server** to limit the flow of biometric information. Also, make sure you have **sole control.**

If you have more than one branch or business establishment, separate databases should be securely stored there if the individuals targeted by your biometric system or process do not need to be identified or authenticated in more than one location.

Be aware that **cloud storage** involves particular issues. If you are considering using cloud services for biometric information, you should analyze this as part of your privacy impact assessment to ensure it provides greater security and confidentiality.

You also have **additional legal obligations** to comply with if you plan to use a service provider located outside of Québec:[23]

> (If you are acting for a public body) Ensure that the data will benefit **from protection equivalent** to that provided by privacy laws in Québec;[24]

[22] On this subject, see the Commission's resources on its website (for public bodies; for businesses).

[23] Note that **as of September 22, 2023, a specific privacy impact assessment will be required for any project involving the communication of personal information outside of Québec.**

[24] Access Act, section 70.1

> (If you represent a private enterprise) Ensure that the information will **not** be **used for purposes inconsistent with the purpose of the collection** or **communicated without the consent** of the individuals concerned except as provided by law (see *Restricting communication* to *third parties).* [25]

For example, you should choose a cloud service provider that stores data **in Québec,** but above all that offers robust and comprehensive security measures.

Regardless of where you store it, if you intend to use cloud services, you should inform persons concerned of this **when obtaining their consent** and **indicate the location(s)** where their biometric information will be stored. **As of September 22, 2023, you will be required to inform the persons concerned of the possibility that their personal information will be communicated outside of Québec.**

Your contract with your cloud service provider should allow you to **maintain control over the data** you entrust to them. You must require from the custodial service provider to provide the elements necessary to ensure **the protection of the biometric information you entrust to them** (including in terms of confidentiality and security). [26]

✓ ***Privacy-enhancing technologies***

The integrity of biometrics is paramount. To ensure this integrity and maintain confidentiality, you must protect biometric information **at all times** (during storage, network transmission, backup operations, etc.). To do so, you can use **privacy-enhancing technologies,** including encryption. Likewise, you should irreversibly transform the information into code in order to prevent the reconstruction of the original image or print.

✓ ***Restricting access***

The biometric information you collect and store should only be **accessible to a limited number of individuals,** such as those whose functions or mandates necessarily require the use of that information.[27]

You should set up **a logging system** to keep track of who is accessing or using biometric information,[28] even if they are third parties (see below) or IT personnel within your organization. This system should include the use of logs to detect any anomalies, including unauthorized access, so as to be able to intervene quickly and stop the intrusion.

[25] Private Sector Act, section 17.

[26] IT ACT, section 26.

[27] IT ACT, section 25; Access Act, section 62; Private Sector Act, section 20.

[28] IT ACT, section 41, para. 2.

✓ ***Restricting communication with third parties***

You must **obtain the express consent** of the person concerned **for any communication of their biometric information to a third party,** unless a specific legislative provision applies.[29]

If you are hiring a third party and this involves access to the biometric information in your custody (through cloud storage, maintenance, etc.), this access should be **framed by strict contractual provisions** emphasizing, among other things, applicable security measures.[30]

2.2.4. Secure and permanent destruction

Once the purpose of collecting the biometric characteristics or measurements has been achieved, **you have an obligation to destroy them**,[31] whether they are in raw format or converted to code. All existing copies of this biometric information must be destroyed during this operation. You must ensure that any third party providing you with services involving access to biometric information also destroys them.

Since this personal information is sensitive, you must use a method of **permanent and irreversible** destruction. You should also ensure that the storage media used to store biometric information **cannot be recovered in any way once destroyed.**

For more information, you can consult the information on destruction on the Commission's website, either for public bodies or businesses (available in French only).

2.2.5. Ensure access and rectification rights

Every person has the **right of access**[32] to their personal information held by your organization. They also have the **right to request the rectification**[33] of this information. In both cases, they must make a written request and verify their identity.[34]

[29] Access Act, sections 59 et seq.; Private Sector Act, sections 13 and 18 et seq.

[30] IT ACT, section 26, para. 2; Access Act, section 67.2; Private Sector Act, section 20.

[31] IT ACT, section 44, para. 3; Access Act, section 73; Private Sector Act, sections 10 and 12.

[32] Access Act, section 83; Private Sector Act, section 27.

[33] Access Act, section 89; Private Sector Act, section 30.

[34] Access Act, section 94; Private Sector Act, section 30.

If you operate an enterprise, you have **the responsibility**[35] **to ensure the exercise of these rights,** even if a third party is responsible for holding personal information on your behalf.[36]

In order to facilitate the process for the persons concerned, you must **appoint a person in charge of the protection of personal information, who oversees, among other things, the handling of requests for access or rectification**.[37] You can also create a dedicated section on your website or provide an email address for these requests. If applicable, provide this information to the persons concerned when obtaining their consent.

✓ ***You must:***

> **Respond promptly** to requests for access or rectification, either verbally or in writing. A public body has 20 days to do so (an extension to up to 30 is possible in some contexts), while a private enterprise has 30 days;

> **Justify any refusal** based on the applicable law (Access Act, Private Sector Act, or other laws containing provisions concerning the protection of personal information);

> **Inform** the person concerned of **the remedies** available before the Commission.

> **Provide the information in a format that is intelligible** to the person concerned, in the event you grant access to it.

Failure to respond within the time limit is tantamount to an alleged refusal on your part. A refusal of access, or a reply which is not to the satisfaction of the person concerned, shall give rise to an appeal (available in French only) to the Commission.

To take this one step further, the Commission makes available to organizations – and the public – privacy-related information in the Guides and Fact Sheets section (available in French only) of its website.

[35] In general, every private enterprise has a legal responsibility to ensure the protection of personal information held by it; see the Private Sector Act, section 3.1.

[36] Private Sector Act, section 16.

[37] Private Sector Act, section 3.1.