ORIGINAL TEXT IN FRENCH

Commission
d'accès à l'information
du Québec

Biometrics: Principles and Legal Duties of Organizations

Practical Guide for Public Bodies and Enterprises

Document last updated in July 2020

INTRODUCTION

The Commission d'accès à l'information (the Commission) promotes and upholds citizens' rights in the area of access to documents held by public bodies and the protection of personal information held by public bodies and enterprises.

In recent years, the Commission has observed **an increase in the use of biometrics**, in both the public and private sectors.

Biometrics have become more easily available as a result of technological progress (algorithms, machine learning, storage capacity, etc.), and can now be installed and maintained more affordably. **Biometric systems** are seen as a simple, practical way of achieving various objectives (tracking of employee time and attendance, identity verification, access to premises, etc.). Some companies even offer **turnkey versions of these systems**, making them easier to implement.

However, this growing popularity has led to **a certain amount of trivialization** with respect to the implications of biometrics for the protection of personal information. While biometric technology is generally regarded as safe, it is all too easy to overlook the fact that its use involves a certain level of **risk to privacy**. In addition, the legal framework governing its use is sometimes misunderstood.

This Guide was produced with this in mind. Its objectives and target audience are described in the pages that follow.

WHAT ARE THE AIMS OF THIS GUIDE?

The Commission has published this Guide:

- to ensure that public bodies and enterprises are **aware of their duties and responsibilities** with respect to the protection of personal information obtained from biometrics;
- to assist public bodies and enterprises with **the task of filling out** the disclosure form for databases of biometric characteristics and measurements (in French only), which must be sent to the Commission before bringing a biometric system into service.

FOR WHOM IS THE GUIDE INTENDED?

The Guide is intended for decision-makers and officers responsible for implementing projects involving biometrics.

Its target audience includes all public bodies and private enterprises, regardless of size.

The legal obligations currently in force in Québec with respect to biometrics apply to **every organization that wishes to use a biometrics system.** These systems require a database of biometric characteristics and measurements, and each organization is responsible for its own database.

In addition, the Guide is intended for **companies supplying biometric solutions**. They must also be familiar with these rules if they are to advise their customers properly without misleading them, and if they are to offer products that comply with current legislation in Québec.

WHAT IS BIOMETRY?

In this Guide, the term **biometry** refers to the set of techniques used to analyze one or more of a person's unique physical, behavioural or biological characteristics in order to establish or prove his or her identity. Identification and authentication processes can now be fully automated thanks to the computerization of biometry, and systems such as these constitute the technology's principal use today.

In some cases, morphological, behavioural or biological characteristics can be used **for purposes other than identification or authentication of individuals**, for example in thermal imaging cameras, anonymous video analytics (AVA), medical alert bracelets and emotional recognition systems.

Although uses such as these are not covered specifically by the principles set out in this Guide, the organizations that implement them must still abide by the provisions of the *Act respecting Access to documents held by public bodies and the Protection of personal information* or the *Act respecting the protection of personal information in the private sector*.

Regardless of the type of project, once it has been established that it requires the use of biometric characteristics and measurements, the organization concerned should **conduct a privacy impact assessment** (document in French only; see the introduction to Section 1), because the characteristics and measurements in question constitute sensitive personal information (see below).

Biometrics categories

There are three main categories of biometrics:

- **Morphological biometrics**, where a person's specific physical traits are analyzed. This category includes, but is not limited to, fingerprints, hand geometry and facial, retinal and eye recognition.
- **Behavioural biometrics**, where a person's behaviours, such as signature recognition, voice print, gait and keyboard strokes, are analyzed.
- **Biological biometrics**, where a person's biological elements, such as DNA, blood, saliva, urine and odour, are analyzed.

The **biometric characteristics and measurements** obtained from these analyses are also referred to as **biometric data** in this Guide.

They are generally collected or recorded in **databases of biometric characteristics and measurements**, i.e. biometric datasets, in raw format (image or print) or compressed format (biometric code or template extracted from an image or print).

Identification and authentication

The principles set out in this Guide apply to all biometric projects designed to achieve one of the following purposes:

- **Identification**, i.e. finding a specific identity from a set of identities stored in a database. The biometric characteristics and measurements of a person whose identity is unknown are compared with those in the database to answer the question: “Who is this person?”
- **Authentication**, i.e. verifying or proving a person’s identity by comparing his or her data “one by one” with the biometric characteristics and measurements of a known person, to answer the question: “Is this person who he or she is claiming to be?”

In this Guide, the term **biometric system** refers to any technological identification or authentication infrastructure that uses a database of biometric characteristics and measurements.

A biometric system is usually divided into two stages of operation:

- **Enrollment or input**, when the biometric characteristics and measurements are entered for the first time and saved in the database
- **Recognition**, when the identification or authentication process described earlier is carried out.

Biometric characteristics and measurements: personal information

Biometric data is **personal information**, i.e. information concerning a natural person which allows the person to be identified[1]. Biometric data are unique, distinctive and persist over time.

This is true of images (of the face, iris, etc.) and prints (fingers, hand geometry, voice, keyboard strokes, etc.), be they static (fixed images or prints) or dynamic (animated images or prints, or images or prints with a time dimension).

This is also true of digital or other **codes (also referred to as templates or models)** that are **derived from the images by means of an algorithm.** A measurement or code constitutes a biometric characteristic or measurement, and if it is stored for the purpose of recognizing the person at a later date, it can also be used to identify that person because of its distinctive nature.

[1] Act respecting access, section 54; Act respecting the private sector, section 2.

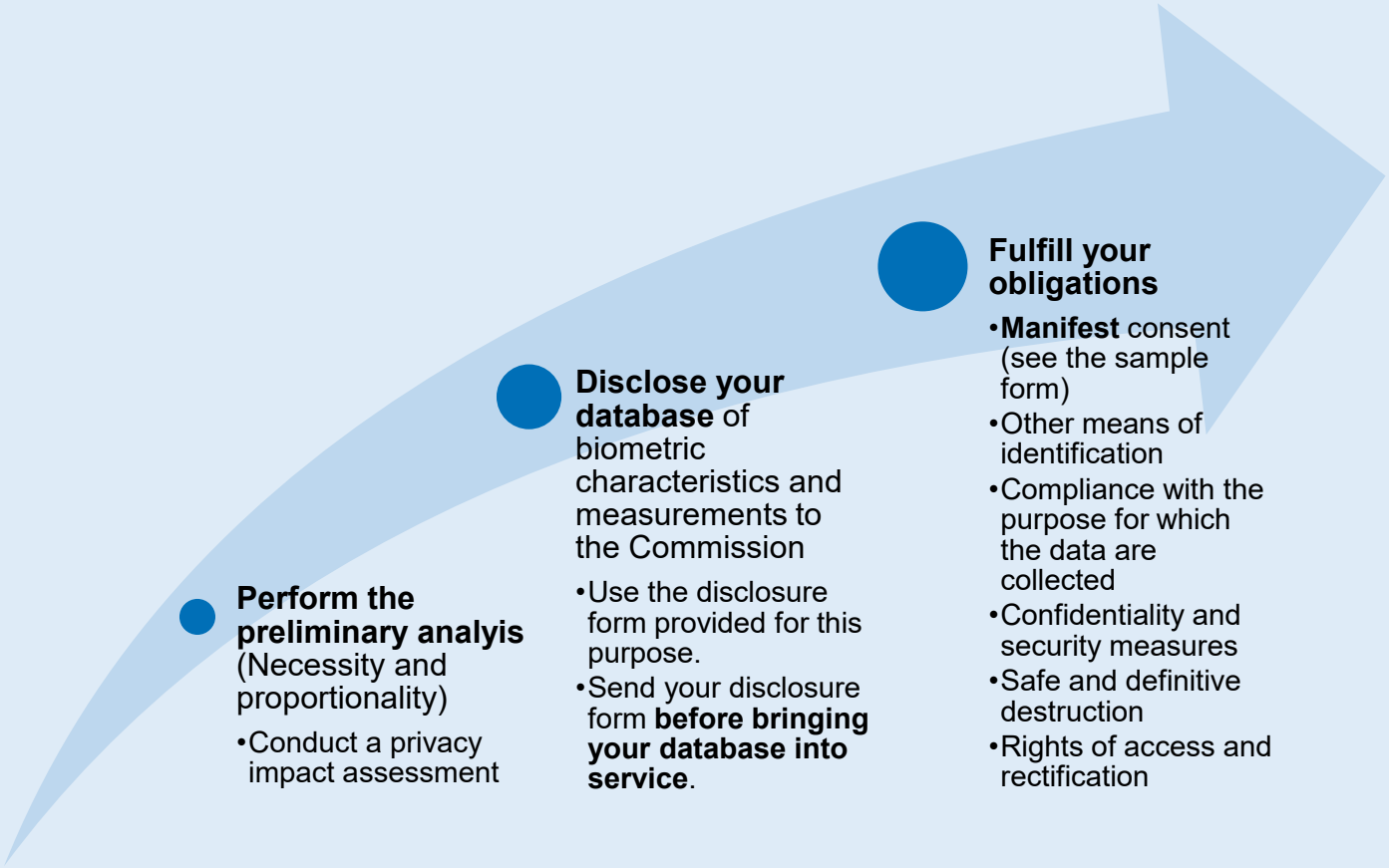
Biometric characteristics and measurements: sensitive information

Biometric data are highly **sensitive**. They are **permanent, distinctive** characteristics, **unique** identifiers composed of highly **personal** information.

Some of these data can also be used to **deduce information other than the person's identity**. For example, a person's iris or gait may reveal the presence of a disease or handicap. Biometric measurements or characteristics may also reveal ethnic origin.

If the confidentiality of biometric data is compromised, the **consequences** for the person concerned can be **extremely serious**. While a magnetic card, personal identification number or password can be replaced, a person cannot change his or her face or fingerprints. **The risks relating to identity theft – among other things – are therefore especially consequential.**

SUMMARY OF THE PROCESS



Contact the Commission if you have questions concerning this Guide, the disclosure requirement or the creation of a database of biometric characteristics and measurements. Please bear in mind that the Commission will not issue a legal opinion:

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

MONTREAL
Bureau 900
2045, Stanley
Montreal (Québec) H3A 2V4
Telephone: (514) 873-4196
Fax: (514) 844-6170

Toll-Free Line
1-888-528-7741

E-mail
cai.communications@cai.gouv.qc.ca

Website
www.cai.gouv.qc.ca

TABLE OF CONTENTS

1. PERFORM THE PRELIMINARY ANALYSIS

For a public body or enterprise, the use of biometrics involves **collecting, using, storing, communicating or destroying highly sensitive personal information**.

You must therefore make a **careful assessment** before implementing a biometric system. To do this, you must understand the applicable rules and consider the sensitive nature of personal biometric information as you assess both the legality of your plans and your obligations if and when you deploy the chosen solution.

The best way of carrying out this assessment (and also a good practice) is to **conduct a privacy impact assessment** (document in French only). The Commission has published a Guide (in French only) for this. You may refer to it during your analysis.

1.1. Comply with the applicable legislation

In Québec, the collection and use of biometric data by public bodies and enterprises is governed by **a number of different laws**. The Commission is responsible for enforcing the provisions applicable to the use of biometry in the following three Acts:

- *Act to establish a legal framework for information technology*[2]
- *Act respecting Access to documents held by public bodies and the Protection of personal information*[3]
- *Act respecting the protection of personal information in the private sector*[4]

Under these Acts, the Commission may **suspend or prohibit the bringing into service** of a database of biometric measurements or characteristics.

It may also **make orders** to determine how a database of biometric measurements or characteristics must be set up, used and consulted, the conditions on which data can be released or retained, and how measurements or characteristics recorded for personal identification purposes are to be archived or destroyed.

Ultimately, the Commission may **order the destruction** of a database if it is not in compliance with its orders or if it otherwise constitutes an invasion of privacy.

Before deciding to implement a biometric system in your organization, and before committing time and money to the project, you must ensure that it complies with the basic principle of necessity.

[2] CQLR, c. C-1.1; hereinafter the Act respecting information technology.
[3] CQLR, c. A-2.1; hereinafter the Act respecting access.
[4] CQLR, c. P-39.1; hereinafter the Act respecting the private sector.

1.2. Collect only the information that is necessary

First and foremost, you must **question the necessity** of collecting personal information, including biometric measurements or characteristics.

The *Act respecting the private sector* and the *Act respecting access* both provide that only personal information that is necessary may be collected[5]. **This rule cannot be circumvented by obtaining permission from the person concerned**.

Necessity of collecting biometric data is assessed using the following criteria:

1.2.1. The purpose for which the information is collected must be important, legitimate and real

Biometry should be used to **resolve a problem situation** – in other words, for an **important and legitimate purpose**.

You cannot simply state the underlying reason for the system (e.g. "to verify identity and hours worked"). On the contrary, you must **specify and document** the problem situation that justifies the use of personal information and biometry.

Examples of problems**:**

- fraud and theft of time;
- a workplace context and environment that makes it very difficult to control arrival and departure times or presence at work;
- the need for enhanced control of access to highly secure premises.

✓ ***Consider the following questions:***

- **Why** is the information being collected?
- What is the **purpose** of using biometrics?
- Is this a **real and practical problem**?

✓ ***You must be able to:***

- **Clearly identify the problem** or situation that you wish to remedy. Utility or convenience ("it's easier, it's more practical") cannot be used to justify the collection of biometric data.
- **Document the scope of the problem** or situation. The problem must be significant and real, as opposed to possible or potential. It must provide a valid reason for collecting such highly sensitive data. You must therefore identify real elements to prove the existence or probability of the problem, and its scope.

[5] Act respecting access, section 64; Act respecting the private sector, sections 5 and 6.

1.2.2. The data collected must be proportional to the purpose

The use of biometrics as a solution must be **proportional** to the purpose for which the data is collected, given the other methods available and the consequences for the people concerned. The highly sensitive nature of biometric data must be considered in your assessment. Collection of this type of data constitutes a significant invasion of individual privacy.

You should consider the following three questions when deciding whether the use of biometrics is an appropriate way of addressing the problem:

✓ ***Will the collection of biometric data achieve the purpose for which the biometric system was created? Is it an effective (rational) and proven way of achieving this purpose?***

- Make sure the proposed biometric system is an **appropriate solution** to the problem you have identified. Document its effectiveness in resolving the situation.
- Consider **the limitations** of the proposed solution. Some biometric systems have error rates that may compromise their effectiveness as a means of achieving your purpose.

✓ ***Is there a less invasive way of achieving the same purpose, other than with a biometric system? Can you minimize the level of invasiveness that would arise from the use of biometrics in your project?***

- Explore **the other methods** available to you for achieving your purpose and for solving the problem situation, other than by using biometrics.
- Identify the methods that **are the least invasive**, including those that do not involve the use of biometrics or that minimize the volume of personal information collected by your organization.
- In what way do these other methods **not allow your organization to achieve its purpose** or solve the problem you have identified? Why is it necessary to use biometrics when these other solutions are available? If you have tested other solutions and they turned out to be ineffective in achieving your purpose, document the situation and, above all, **explain why the other solutions were not effective or appropriate**.
- If there is no other reasonably effective way of achieving your purpose, one that does not constitute an invasion of individual privacy, identify **ways in which the invasion of privacy** can be minimized in your project. What steps can you take to reduce the risk involved in collecting personal information?

Examples of steps that can be taken to reduce the risk:

- Collect only the algorithmic code extracted from a fingerprint, rather than the raw image.

- Use a decentralized storage system.
- Implement stringent confidentiality measures.

✓ ***Are the benefits of using biometrics more important than the invasion of individual privacy and the consequences that may arise from the use of a biometric system?***

- **Document the advantages** of using biometrics to achieve your purpose.
- **Document the disadvantages** and risks to privacy or the protection of personal information, along with the other potential consequences. Consider all the consequences that are likely to arise.

Examples of consequences:

- Infringements of other rights.
- Consequences of incidents affecting data confidentiality (e.g. identity theft).

- **Weigh the advantages and disadvantages** of the proposed biometric system.

1.3. When your analysis is complete…

If your assessment **does not lead to the conclusion** that the use of biometric data is both necessary and proportional…

- **Your project does not comply with the applicable legislation.** Consider the possibility of changing your project to make it compliant, and then disclose it to the Commission. Otherwise, you must find another solution.

If you come to the conclusion that it is **necessary** to collect biometric characteristics and measurements:

- **You may collect only the data that is essential to prove or verify identity**.
- The law provides that a person's identity can only be verified by using **the minimum number** of characteristics and measurements needed to link the person to the act.[6] For example, if one single fingerprint is sufficient to identify a person, you should not collect fingerprints from all ten fingers.
- You must **disclose your project** to the Commission.

To continue with the process, you must meet a certain number of obligations, which are described in the next few pages of the Guide.

[6] Act respecting information technology, section 44.

2. UNDERSTAND AND MEET YOUR OBLIGATIONS

2.1. *Before* implementation of a biometric system

2.1.1. Disclose the database of biometric characteristics and measurements to the Commission

Before proceeding with your project, you must **disclose** it to the Commission[7] if it involves the creation of a database of biometric characteristics and measurements.

Use the form (in French only) provided, which is available on the Commission's website. You must complete the form *before you bring your database into service* and submit it in plenty of time for the Commission to examine it.

It is preferable from both a legal and financial standpoint to do this well in advance, so that you do not spend money unnecessarily on database design, overhaul or destruction if the project is deemed to be non-compliant.

If your project does not comply with the legislation or otherwise infringes individual privacy, the Commission may **prohibit you from bringing it into service**, make an **order requiring you to make changes to your project** or **order you to destroy your database**.

If your database of biometric characteristics and measurements already exists but you have not disclosed its existence to the Commission, **you must do so** as quickly as possible.

2.2. *During* implementation of a biometric system

(i.e. when you begin to use the system with the people concerned)

2.2.1. Obtain manifest consent from the people concerned and provide for another means of identification if they refuse

The law prohibits you from **requiring** that a person's identity be verified or confirmed by means of a process that allows biometric characteristics and measurements to be recorded.[8] This means that:

- You must obtain **valid, manifest consent** from every person concerned.

[7] Act respecting information technology, section 45.
[8] Act respecting information technology, section 44.

- You must **provide for an alternative solution** to verify or confirm a person's identity if he or she refuses to give or withdraws consent.
- You cannot use biometric characteristics and measurements **without the knowledge** of the person concerned (i.e. data obtained without the person's knowledge).

✓ ***Manifest consent***

Consent is described as "manifest" when it is **explicit and unequivocal**. To give manifest consent, a person must perform a positive action that clearly demonstrates his or her agreement. The opposite of manifest consent is usually tacit or implicit consent, which is inferred from a person's behaviour, conduct or actions.

The best way of giving manifest consent is to **sign a document**. If necessary, a signed document will also serve to show that the obligation to obtain consent has been met.

The fact of obtaining consent **does not release you from your obligation** to collect only the personal information that is necessary (see the detailed analysis in section **Erreur ! Source du renvoi introuvable.**).

✓ ***Free, enlightened consent given for a specific purpose and for a limited time***

For consent to be legally valid in accordance with the principles set out in the legislation respecting the protection of personal information,[9] it must be:

- **Free:** The person's decision must not be influenced by undue constraint or pressure (e.g. threats, financial or other incentives, etc.). A person may withdraw his or her consent at any time.
- **Enlightened:** The person must have enough information to understand the scope of what is being consented to. You must therefore provide **all** the relevant information:[10]
  - the purpose of the biometric system;
  - the biometric characteristics and measurements that will be collected;
  - the procedure used to collect the biometric characteristics and measurements;
  - the other personal information that will be collected and used in association with the biometric data;
  - the use that will be made of the biometric data and personal information;
  - the categories of people who will have access to the data and information within the organization;
  - the security measures applied to protect the data and information (e.g. encryption, storage location, depersonalization, etc.);

[9] Act respecting the private sector, section 14. These same criteria are also applied in the public sector.
[10] Among other things see the Act respecting access, section 65 and the Act respecting the private sector, section 8.

- the rules governing future communication of the data and information;
- the length of time for which the data and information will be kept;
- how the right of access and rectification can be exercised;
- the possibility that the person may refuse to provide biometric characteristics and measurements and use another means of identification.

You must present this information **clearly**, in a way that is **easy to understand,** using **simple but precise terminology** so that everyone concerned understands the scope and consequences of their consent. Do not use overly complex legal language.

> **Specific:** The **scope** of the consent must be **clearly defined** and must be related to the purpose for which the biometric system will be used. Avoid formulating your request in general or imprecise terms using expressions such as "any information deemed necessary."

> **For a limited time:** Consent is given for a **defined period of time**, expressed either as a duration (e.g. number of months) or in terms of an event or situation (e.g. when the employment relationship ends). Avoid requesting extended consent by using expressions such as "for as long as necessary."

Regardless of how you obtain consent, **be thorough** by providing people with the information they need and by **taking your time** with this crucial step in the process.

A sample consent form (in French only) is available on the Commission's website. It **must be adjusted** to the specific features of the biometric system proposed by your organization.

✓ ***Authentication during enrollment***

When individuals have consented to the use of the biometric system, you must confirm their individual identities before enrolling their biometric data in the database. The most common way of verifying a person's identity is to use identity documents. The Commission invites you to consult its information sheet for enterprises (in French only), which contains important clarifications concerning the ways in which identity documents should be used. In short, **you may ask to see the documents, but it is usually not necessary to collect their content** in any way whatsoever.

If you collect other personal information during enrollment, you must make sure the information you collect is necessary (see section **Erreur ! Source du renvoi introuvable.**), and you must also comply with your regular legal duty to protect personal information.

✓ ***Identification method if consent is not given***

The requirement to obtain manifest consent before using biometric characteristics and measurements to identify a person means that you cannot impose a biometric system. The people concerned should not be **pressured or inconvenienced** by their choice. You

must therefore provide an alternative solution for people who do not give or who withdraw their consent.

Examples of alternative solutions:

- Access card system
- Use of unique authentication tokens
- Use of a password or identity code

✓ ***No collection of biometric data without the person's knowledge***

The law prohibits the use of biometric characteristics and measurements to identify or verify a person's identity **without his or her knowledge.**[11] This is similar to the obligation to obtain manifest consent, and in most cases means that you must collect biometric characteristics and measurements **directly from the person concerned.**

2.2.2. Use the data only to achieve the purpose for which it was collected

The biometric data you collect must be used **solely** to achieve the original purpose for which the biometric system was created,[12] i.e. for identification or authentication (except in the cases provided for by law). This obligation is all the more important because of the highly sensitive nature of biometric data.

For example, you must **avoid discrimination** that may result from the discovery of other information revealed by the biometric characteristics and measurements. Among other things, you must not make a decision concerning a person based solely on his or her biometric data.[13]

2.2.3. Apply confidentiality and security measures

Remember: biometric data are highly sensitive because they are unique, distinctive and personal. They may therefore be an attractive target for hackers and must be protected by **strong confidentiality and security measures** tailored to the volume and distribution of the data and the medium on which they are stored.[14]

You are responsible for the database of biometric characteristics and measurements, and must establish these measures according to the context in which it is used. **Different methods must be used to ensure physical, technological, logical and organizational security**.

[11] Act respecting information technology, section 44.
[12] Act respecting access, section 65.1; Act respecting the private sector, section 12.
[13] Act respecting information technology, section 44, para. 2.
[14] Act respecting information technology, sections 40 and 41; Act respecting access, sections 53, 62 and 63.1; Act respecting the private sector, sections 10 and 20.

To ensure that biometric data are stored securely and to maintain their confidentiality, your measures must focus on the data format, the storage medium, the server's location, privacy enhancement technology, and restrictions on access by and communication to third parties.

✓ ***Data format***

You must give **preference to systems that irreversibly converts** images or prints **into code**. This limits the sensitivity of the biometric characteristics and measurements that are collected and stored. Once the algorithmic conversion process has been completed, it should be impossible to restore the original image or print.

In the first place, this prevents the image or print from being reused for purposes other than those for which it was collected. In the second place, it provides the person concerned with an assurance that if the data are lost or stolen, the biometric identifiers cannot be used directly to usurp his or her identity in another biometric system.

✓ ***Storage medium***

Storage of biometric data may be **centralized** in a single database. In this case, all the data are kept together, meaning that a security breach (unauthorized access, leaked information, etc.) will have very significant consequences.

Wherever possible, you should opt instead for a **decentralized** storage solution to mitigate this risk. An example would be an external, individual or portable medium under the control of the person concerned, on which biometric characteristics and measurements are stored after being encrypted or converted into code.

✓ ***Server location***

If you must create a centralized database, it should be stored **locally on a secure server**, to limit the circulation of biometric data. Also make sure you have **exclusive control** of the server.

If you have several branches or business establishments, separate databases can be kept securely in each location if the people concerned do not need to be identified or authenticated at several different places.

The Commission recommends that cloud-based storage solutions should not be used for biometric data, given the particular issues (document in French only) associated with this type of technology. However, if you feel this solution would be more secure and more likely to ensure data confidentiality, you should consider it in your privacy impact assessment.

You must also meet a number of **legal obligations** if you are considering a service provider located outside Québec:

- (if you are acting on behalf of a public body) make sure the data will receive protection **equivalent to that** provided for by Québec's current legislation respecting the protection of personal information;[15]
- (if you are acting on behalf of an enterprise) make sure the data will **not be used for purposes incompatible with the purpose for which they were collected, and that they will not be communicated without the consent** of the people concerned, except in the cases provided for by law (see *Restricted communication to third parties*).[16]

You should therefore choose a service provider that uses cloud-based storage **in Québec**.

Regardless of the storage location, if you intend to use cloud storage services, you should inform the people concerned **at the time you obtain their consent** and you should **state where** their biometric data will be stored.

Your contract with your cloud storage provider must give you **control over the data** entrusted to the provider. You must ask the provider for guarantees regarding **the protection of the biometric data entrusted to them** (in particular with regard to confidentiality and security).[17]

✓ ***Privacy-enhancing technologies***

The integrity of biometric data is essential. To ensure their integrity and confidentiality, you must protect biometric data **at all times** (during storage, during transmission via a network, during backups, etc.). **Privacy-enhancing technologies** including encryption can be used for this purpose. Similarly, you must convert the data irreversibly into code, so that the original image or print cannot be reconstructed.

✓ ***Restricted access***

The biometric data you collect and store should be accessible only to **a limited number of people**, those whose duties or work necessarily require them to use the data.[18]

You must set up a **logging system** for database access, so as to keep track of the people who consult or use the biometric characteristics and measurements,[19] regardless of whether they are third parties (see below) or employees responsible for information technology within your organization. The system must use computer logs to detect anomalies such as unauthorized access, so that quick action can be taken to deal with intrusions.

[15] Act respecting access, section 70.1
[16] Act respecting the private sector, section 17.
[17] Act respecting information technology, section 26.
[18] Act respecting information technology, section 25; Act respecting access, section 62; Act respecting the private sector, section 20.
[19] Act respecting information technology, section 41, para. 2

✓ ***Restricted communication to third parties***

You must **obtain manifest consent** from the person concerned before **communicating his or her biometric data to a third party**, unless the communication is covered by a specific legislative provision.[20]

If you use the services of a third party, and if those services require access to biometric data held by you (e.g. cloud storage, biometric system maintenance, etc.), access must be **governed by strict contractual provisions** emphasizing the applicable security measures.[21]

2.2.4. Destroy the data permanently and safely

When the purpose for which the biometric characteristics and measurements were collected has been achieved, **they must be destroyed,**[22] regardless of whether they are in raw or converted format. All existing copies of the biometric data must be destroyed during the operation. You must ensure that any third parties providing services requiring access to the database also destroy the data in their possession.

Because of the sensitive nature of the data, you must use a **permanent, irreversible** method of destruction. You must also clean up the storage media used, to ensure that the biometric data **cannot be recovered in any way whatsoever**.

For additional information, please refer to the Commission's datasheet on *the destruction of documents containing personal information*.

2.2.5. Uphold the right of access and rectification

Every person has a **right of access**[23] to the personal information concerning him or her that is held by your organization. He or she also has the **right to request rectification**[24] of the information. In both cases, the person must submit a request in writing and prove his or her identity.[25]

If you operate an enterprise, it is **your responsibility to ensure that these rights can be exercised,** even if the information in question is held by a third party on your behalf.[26]

To facilitate the process, you may **appoint someone to be in charge of requests for access or rectification.** You may also create a dedicated section on your website or set

[20] Act respecting access, sections 59 and following; Act respecting the private sector, sections 13 and 18 and following.
[21] Act respecting information technology, section 26, para. 2; Act respecting access, section 67.2.; Act respecting the private sector, section 20.
[22] Act respecting information technology, section 44, para. 3; Act respecting access, section 73; Act respecting the private sector, sections 10 and 12.
[23] Act respecting access, section 83; Act respecting the private sector, section 27.
[24] Act respecting access, section 89 and following; Act respecting the private sector, section 30.
[25] Act respecting access, section 94; Act respecting the private sector, section 30.
[26] Act respecting the private sector, section 16.

aside an e-mail address specifically for these requests. Where applicable, this information should be given to the people concerned when you obtain their consent.

✓ ***You must:***

- **Respond diligently** to requests for access or rectification, regardless of whether they are made verbally or in writing. A public body has 20 days to do this (and can extend this period to 30 days in some situations), while a private enterprise has 30 days.
- **Give reasons** for refusing a request, based on the applicable legislation (*Act respecting access, Act respecting the private sector* or other legislation containing provisions relating to the protection of personal information).
- **Inform** the person concerned that he or she may **have recourse** to the Commission.
- If you grant access, **provide the information in a format that is easy for the person to understand**.

If you fail to respond within the time permitted, you are assumed to have refused the request. If you refuse a request or if your response is deemed unsatisfactory, the person concerned may file an application or complaint (page in French only) to the Commission.

For additional information, the Commission's website offers a number of publications and documentation in English.