



<i>Policy No. :</i>	A20231021	Personal Data Protection	
<i>Revision :</i>	1		
<i>Owner :</i>	Christophe Hayart		
<i>Approval :</i>	Jacques Beauchemin	<i>Date :</i> November 9 2023	

# Policy – Personal Data Protection

## Contenu

1	Definition of key terms .....	2
2	Management Commitment.....	4
3	Personal Information Used at AFT.....	5
4	General Flow Chart for Confidential Personal Information Processing.....	5
5	Continuous Improvement.....	6
6	Guidelines and Technological Development.....	6
7	Handling requests and complaints relating to privacy.....	7
8	Confidentiality Incident Management.....	8

<i>Policy No. :</i>	A20231021	Personal Data Protection	
<i>Revision :</i>	1		
<i>Owner :</i>	Christophe Hayart		
<i>Approval :</i>	Jacques Beauchemin	<i>Date :</i>	November 9 2023

# 1 Definition of key terms<sup>i</sup>

## Personal Information

Personal information is information that allows a natural person to be identified, directly or indirectly. Personal information is confidential. Their confidentiality arises from the right to privacy, allowing any person to exercise control over the use and circulation of their information.

Please note that the Commission considers that:

*Information generated using artificial intelligence systems, including inferred information, is personal information subject to applicable laws.*

Depending on the context, personal information may be:

- Sensitive
- Depersonalized
- Anonymized

## Public Information

Some information that directly identifies individuals is public. Please note that information concerning the exercise of a function of a person within a company or a public body such as:

- name;
- title;
- function;
- email, address and telephone number of their place of work  
are public.


## Sensitive Personal Information

Personal information is sensitive when it gives rise to a high degree of reasonable expectation of privacy, due to its nature or the context of its use. Information is considered sensitive if it is:

- Medical;
- Biometric;
- Otherwise intimate.

For example, sensitive information may concern:

- Health or sexual orientation;
- Morphological, behavioral or biological characteristics (biometrics);
- The ethnic group;
- Philosophical or religious beliefs;

<i>Policy No. :</i>	A20231021	Personal Data Protection	
<i>Revision :</i>	1		
<i>Owner :</i>	Christophe Hayart		
<i>Approval :</i>	Jacques Beauchemin	<i>Date :</i>	November 9 2023

- The state of finances.

## Depersonalized or anonymized personal information

As a representative of a public organization or company, you are responsible for ensuring the confidential management of personal information, from its collection to its destruction. This concerns the applicable laws.

When the purpose for which you collected personal information has been accomplished, you immediately have an obligation to securely destroy it. The only restriction on this destruction obligation: the period provided for by law or by a retention schedule established by government regulation (e.g.: for tax obligations).

As of September 22, 2023, applicable laws provide an alternative to the destruction of personal information. Depending on the fulfillment of the purpose of their collection, it will be possible to keep them by anonymizing them to use them for purposes of public interest (for public organizations) or serious and legitimate purposes (for companies):

**Information concerning a natural person is anonymized when it is, at all times, reasonable to predict in the circumstances that it no longer allows, in an irreversible manner, to directly or indirectly identify that person.**

Caution and vigilance are required if you intend to anonymize personal information in this context. This is a complex process that must ensure the impossibility of re-identification of a natural person by any type of technological means.

In addition, to be able to be preserved rather than destroyed, the information must be anonymized according to generally recognized best practices and according to the criteria and methods determined by government regulation. In the absence of government regulations, it is therefore not possible to anonymize information in order to preserve it and use it for public interest or serious and legitimate purposes.


The public body or company that collects personal information must develop and implement governance rules governing, in particular, its destruction. These rules must also refer to anonymization, where applicable.

### **The opinion of the Quebec Commission for Access to Information on anonymization:**

In light of current and future technological advances, the Commission considers that it is almost impossible to certify that anonymized information could not possibly be reidentified.

Some information is so distinctive in nature that it cannot be adequately anonymized. Let's think, for example, of genetic, biometric or even geolocation information.


The anonymization of personal information presupposes risks of confidentiality incidents. The law also provides sanctions for anyone who attempts to identify a person based on anonymized information.

<i>Policy No. :</i>	A20231021	Personal Data Protection	
<i>Revision :</i>	1		
<i>Owner :</i>	Christophe Hayart		
<i>Appoval :</i>	Jacques Beauchemin	<i>Date :</i>	November 9 2023

## 2 Management Commitment

At AFT, we are committed to working with all employees to meet legal requirements, eliminate the misuse of confidential personal information and reduce the risk of data protection breaches. Based on clear responsibilities and processes and their regular audits, AFT will continue to dedicate resources to improve its data security protocols and thus improve the protection of the confidential personal information of its employees, customers and business partners. To this end, AFT has created a Personal Data Protection Committee (PDPC) composed of:

- CEO and Chief Privacy Officer
- Director, Marketing, AFT Global; responsible for assessing global data risks and data integrity on AFT's website and customer management software.
- Director, Information Technologies, AFT Global; responsible for the integrity of computer systems.
- Total Quality Director, AFT Global; Chairman of the Personal Information Protection Committee.
- Director of Human Resources, AFT Oy; is responsible for regional personal information protection legal compliance.
- Director of Human Resources, AFT Inc., is responsible for regional personal information protection legal compliance.

<i>Policy No. :</i>	A20231021	Personal Data Protection	
<i>Revision :</i>	1		
<i>Owner :</i>	Christophe Hayart		
<i>Approval :</i>	Jacques Beauchemin	<i>Date :</i>	November 9 2023

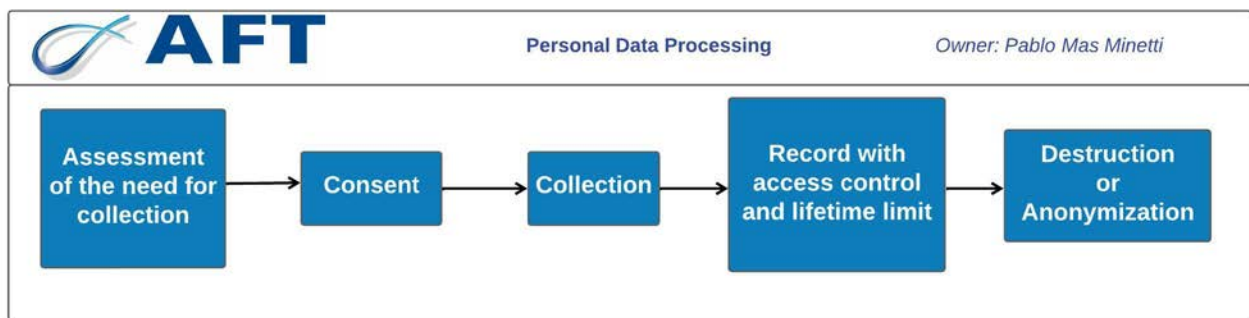
### 3 Personal Information Used at AFT

AFT uses several types of personal information necessary for its business processes. Some of its information is considered sensitive and is therefore subject to stricter use and consultation measures. Any employee with access to the following types of information must ensure that they understand and observe the process for processing this information by reviewing it with their manager or one of the members of the committee.


- Photo
- Government identification number (e.g. passport, SIN, PIN, GST, QST, etc.)
- Banking information
- Medical information
- Intimate information
- All information defined as sensitive by law; consult section 1.3 of this document and the website of the *Commission d'accès à l'information du Québec* as a reference.

### 4 General Flow Chart for Confidential Personal Information Processing

For each of the systems processing confidential personal information, a system manager is assigned, a flow chart for collection and processing is defined and a risk assessment is conducted by the PDPC based on each of the critical processing steps. data shown below:



All confidential personal information is collected and retained only when necessary for AFT's business processes. Unless there are specific legal obligations, when the purpose for which the information was collected is accomplished, this information is destroyed.

<i>Policy No. :</i>	A20231021	Personal Data Protection	
<i>Revision :</i>	1		
<i>Owner :</i>	Christophe Hayart		
<i>Appoval :</i>	Jacques Beauchemin	<i>Date :</i>	November 9 2023

## 5 Continuous Improvement

As part of its new obligations, AFT has completed a complete inventory of its computer systems likely to contain personal information. A risk analysis was then conducted to increase control of personal information on several systems. This risk analysis has already generated several additional rules and measures in the processing of personal information. Furthermore, to meet its legal obligations, ensure the maintenance of these rules and improve its control of information, AFT undertakes to regularly review its policies and processes according to the following continuous improvement plan:

- Internal audits, risk analyses, assessment of private life factors
- Review of incidents
- Correction plan (training, communications)
- Updating processes and their documentation


## 6 Guidelines and Technological Development

*Before collecting personal information, any company representative must ensure that this information is necessary to achieve the objectives determined before collection. A company cannot, even with the consent of a person, collect personal information that is not necessary for the purpose of the matter. Indeed, when it comes to the collection of personal information, the watchword is truly "necessity" and the burden of demonstrating this is on the company. In case of doubt, information is deemed not necessary. When the collection of personal information is necessary, it must be done with transparency and consent.<sup>i</sup>*

The use of traditional documents such as Excel spreadsheets, Word and Adobe documents and particularly their exchange by email represents significant challenges for the control of confidential personal information. Gradually, with the arrival of several new collaboration software and new business management software, AFT is committed to reducing as much as possible the multiplication of files and the sending of files by email. This commitment is necessary to be able to continue to meet the new legal requirements of Law 25 and thereby improve its control of information critical to the smooth running of its business processes.

In this first version of a comprehensive policy on the protection of personal information. AFT asks employees to observe the following rules:

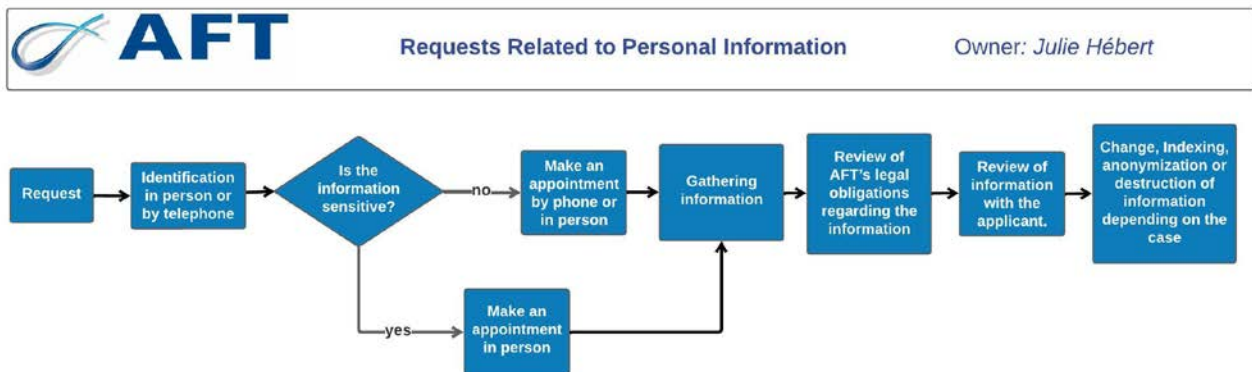
- Use confidential personal information in email communications or documents only when strictly necessary.
- Secure, using a password, all documents containing confidential personal information sent by email.
- To control and limit access to all documents containing confidential personal information.


<i>Policy No. :</i>	A20231021	Personal Data Protection	
<i>Revision :</i>	1		
<i>Owner :</i>	Christophe Hayart		
<i>Appoval :</i>	Jacques Beauchemin	<i>Date :</i>	November 9 2023

- Explore tools other than Outlook to store/organize or archive confidential personal information or documents containing confidential personal information. This information should be organized on other tools currently or soon accessible to employees when they are essential to the company's business processes and destroyed if they are not:
  - AFT shared servers with limited access
  - SmartSheet
  - Epicor
  - DocStar
  - CCMS

## 7 Handling requests and complaints relating to privacy

All requests and complaints relating to privacy will be handled by the human resources department, according to the following process:

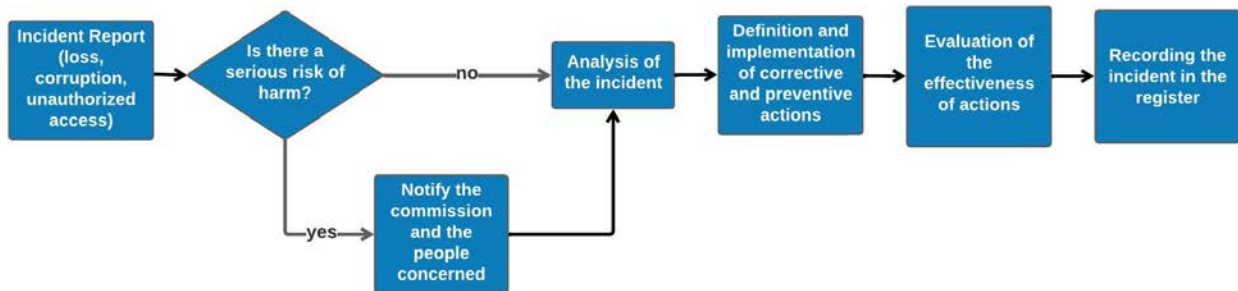


<i>Policy No. :</i>	A20231021	Personal Data Protection	
<i>Revision :</i>	1		
<i>Owner :</i>	Christophe Hayart		
<i>Appoval :</i>	Jacques Beauchemin	<i>Date :</i> November 9 2023	

## 8 Confidentiality Incident Management

All confidentiality incidents will be handled by the IT department and recorded using the following process:

	<b>Confidentiality Incident</b>	<i>Owner: José Cloutier</i>
-----------------------------------------------------------------------------------	---------------------------------	-----------------------------



<sup>i</sup> Reference: website of *Commission d'accès à l'information du Québec*  
<https://www.cai.gouv.qc.ca/quest-ce-un-renseignement-personnel/>