	ADMINISTRATIVE POLICY	<b>PA-RH-146</b>
	<b>Protection of personal information</b>	Date : 22 sept 2023 Version : 1 Page : 1

Issuing department:	Human resources	Written by:	Julie Dunn
Recipient (who):	Employees, candidates and Stakeholders of FMA	Frequency (When):	

## **Introduction**

In the course of your employment, FMA (the "Company") processes personal information about its employees and job applicants. As such, the Company recognizes the importance of respecting privacy and protecting the personal information it holds.

The scope of this procedure covers the entire life cycle of personal information, from collection to destruction. It concerns all employees, candidates, other persons concerned, and stakeholders involved in the collection, processing, retention, destruction, and anonymization of personal information in accordance with legal requirements and good privacy practices.

## **Objective**


The purpose of this policy is to ensure the protection of the privacy of the persons concerned and to comply with legal obligations regarding the protection of personal information.

## **Normative framework**

This policy is governed by Bill 25 (Act respecting the protection of personal information in the private sector). In accordance with this Act, the current policy is available on the Company's website.

## **Definitions**

- **Personal information:** Any information that directly or indirectly identifies a physical person.
- **Life cycle:** all the steps involved in processing personal information, i.e., its collection, use, disclosure, retention, and destruction.
- **Privacy incident:** means any consultation, use or communication of personal information that is not authorized by law, or any loss or other breach of the protection of such information.
- **Law:** refers to the personal information protection law.

	ADMINISTRATIVE POLICY	<b>PA-RH-146</b>
	<b>Protection of personal information</b>	Date : 22 sept 2023 Version : 1 Page : 2

- **Concerned individual:** refers to a physical person which provided the personal information to the Company.
- **Policy:** refers to the policy framework for the governance of personal information.
- **The person responsible:** Human Resources Department

## Responsibilities

The company:

- Takes reasonable measures to reduce the risk of harm being caused to the persons concerned and prevent further incidents of the same nature from occurring.
- Notifies the *Commission d'accès à l'information du Québec* and the person concerned if an incident occurs that could result in serious prejudice.
- Keeps a register of incidents, a copy of which must be sent to the *Commission d'accès à l'information du Québec* at its request.
- Follow up on compliance requests issued by the *Commission d'accès à l'information du Québec*.


## Life cycle

### 1- Collect

Personal information is collected from the concerned individual. When you contact the Company (by phone or e-mail), we collect the following data: your name, phone number/email address, subject and message, and any other relevant information you wish to include.

There are 2 levels of personal information collection from employees and candidates:

- **1st level:** When you apply via a Curriculum Vitae or our Job Application Form, we initially collect the following data: your first and last name, your address, your telephone number, your e-mail address, your date of birth, a summary of your training, your professional experience, etc. All of this is required for the 1st stage of the application process. This is all required for the 1st stage of the application process. This data is needed to determine whether you meet all the criteria (legal working age, required experience) and then to enable us to communicate with you. The data on our Application Form may vary depending on the nature and type of position.
- **2nd level:** If we enter the 2nd stage of the application process (in view of the job offer), we will then need further information for tax and security reasons, such as social insurance number, health insurance number, gender, emergency contacts, preferred language of communication, Canadian citizenship or work permit, work permit, cancelled cheque and general health condition. These details will be added to Ceridian's Dayforce payroll system at the time of hiring.

	ADMINISTRATIVE POLICY	<b>PA-RH-146</b>
	<b>Protection of personal information</b>	Date : 22 sept 2023 Version : 1 Page : 3

## 2- Use and communication

The Company uses and communicates personal information only for the purposes for which it was collected. However, it may change these purposes with the prior consent of the person concerned.

It may also use them for other purposes without the consent of the person concerned, in any of the following cases:

- When the use is for purposes compatible with those for which the information was collected.
- When the use is clearly for the benefit of the person concerned.  
When the use is necessary for the application of a law in Quebec, whether or not such use is expressly provided for by law.
- When use is necessary for statistical purposes and the information is depersonalized, where applicable.

The Company is responsible for maintaining your data and uses Ceridian's Dayforce system for production, scheduling, payroll, government statements, etc. This system is the provider for our payroll system and handles your data securely and confidentially.


The Company complies with all applicable laws and regulations, including the Privacy Act. The information you share with us is strictly confidential and is never disclosed to other parties, unless you have given your prior written consent (e.g., group insurance forms, references, confirmation of employment, etc.).

Any employee may at any time request to consult, correct or delete personal data directly in the Dayforce system using his or her personal access, or request assistance from the Human Resources Department team. To do so, the person concerned must submit a written request by e-mail or physical mail, addressed to the employee in question in the Human Resources Department (Annex 1).

## 3- Storage

If you submit the completed application form and/or your CV, we will not retain your personal data any longer than necessary (as indicated in the privacy and confidentiality clause on the application form) unless you are still being considered for employment.

If you apply for a job and a position with us, you must accept our privacy policy. We apply a retention period of 12 months, although it is possible for employees to delete their data themselves at any time directly on the Dayforce platform or by contacting the person responsible (address on the company website).

	ADMINISTRATIVE POLICY	<b>PA-RH-146</b>
	<b>Protection of personal information</b>	Date : 22 sept 2023 Version : 1 Page : 4

#### 4- Destruction

Your privacy is important to us. That's why we have implemented security measures to prevent theft, loss or other illegal use of your personal data.

All paper documents are kept under lock and key in the Human Resources department. Only human resources staff can remove your physical file from the filing cabinet. The exchange of information via our website is secure and encrypted.

Employees who have access to your personal data are bound by a confidentiality clause and have access to your personal data only if necessary for the performance of their duties.


At the end of employment, employee information is kept in a closed filing system for 2 years, for access to files as needed. They are then sent to Iron Mountain for archiving. Information is kept confidential through this firm.

For candidates who have completed the application form and have not started the 2nd stage of the application process, data will be kept for 12 months, as indicated in the commitment and confidentiality clause of the form in question.

#### Complaint

Any incident involving personal information (unauthorized use/disclosure or loss of personal information) may be the subject of a complaint. (See Annex 2 - Complaint handling procedure)

Approved by:	Julie Dunn	
Date (J/M/A)	Nature of the modification	Version
22/09/23	Creation	1

	ADMINISTRATIVE POLICY	<b>PA-RH-146</b>
	<b>Protection of personal information</b>	Date : 22 sept 2023 Version : 1 Page : 5

## Annex 1

### **Steps when making a request to obtain or modify your personal information.**

**a. Receipt of request**

- i. Once the request has been received, an acknowledgement of receipt is sent to the person concerned to confirm that his/her request has been considered.
- ii. The request must be processed within thirty (30) days of receipt.

**b. Verification of identity**

- i. Before processing the request, the identity of the person concerned must be verified in a reasonable manner. This may be done by requesting additional information or by verifying the identity of the person concerned in person.
- ii. If identity cannot be satisfactorily verified, the organization may refuse to disclose the requested personal information.

**c. Responding to incomplete or excessive requests**

- i. If a request for access to personal information is incomplete or excessive, the Privacy Officer will contact the person concerned to request additional information or clarification.
- ii. The organization reserves the right to refuse a request if it is manifestly abusive, excessive or unjustified.

**d. Processing the request**


- i. Once the identity has been verified, the person responsible for the protection of personal information for processing requests for access to personal information will proceed to collect the requested information.
- ii. The person responsible consults the relevant files to collect the requested personal information, taking care to respect any legal restrictions.

**e. Review of information**

- i. Before communicating personal information to the concerned individual, the person in charge carefully examines the information to ensure that it does not contain any third-party information that is confidential or likely to infringe other rights.
- ii. If third-party information is present, the person in charge assesses whether it can be dissociated or whether it should be excluded from disclosure.

**f. Disclosure of information**

- i. Once the verifications have been completed, the personal information is communicated to the person concerned within a reasonable period of time, in accordance with the legal requirements in effect.
- ii. Personal information may be communicated to the person concerned by electronic means, by secure postal mail or in person, depending on the preferences of the concerned individual concerned and the appropriate security measures.

	ADMINISTRATIVE POLICY	<b>PA-RH-146</b>
	<b>Protection of personal information</b>	Date : 22 sept 2023 Version : 1 Page : 6

**g. Monitoring and documentation**


- i. All steps in the process of handling a request for access to personal information must be recorded accurately and completely.
- ii. The details of the request, the actions taken, the decisions made, and the corresponding dates must be recorded in an access request tracking register.
  - 1. Date request received.
  - 2. Date of acknowledgement of receipt.
  - 3. Date of identity verification.
  - 4. Date of communication of information (if applicable).

**h. Privacy policy**

- i. All personnel involved in processing requests for access to personal information must respect confidentiality and data protection.

**i. Complaints and appeal management.**

- i. If an individual is dissatisfied with the response to his or her request for access to personal information, he or she must be informed of the complaint procedures and recourses available before the *Commission d'accès à l'information*.
- ii. Complaints must be handled in accordance with internal complaint management policies and procedures (Annex 2).

	ADMINISTRATIVE POLICY	<b>PA-RH-146</b>
	<b>Protection of personal information</b>	Date : 22 sept 2023 Version : 1 Page : 7

## Annex 2

### Complaints Handling Procedure

#### 1- Receipt of complaints

Complaints may be submitted in writing, by e-mail or by physical mail. They must be recorded in a centralized register, accessible only to the Human Resources Department staff.

#### 2- Preliminary assessment

The designated responsible person reviews each complaint to assess its relevance and seriousness.

Complaints that are frivolous, defamatory or have no obvious basis may be rejected. However, a justification must be provided to the complainant.

#### 3- Investigation and analysis

The person responsible for the complaint conducts a thorough investigation by gathering evidence, interviewing the parties concerned and collecting all relevant documents.

The person responsible must be impartial and have the necessary authority to resolve the complaint.

The person responsible must maintain the confidentiality of information relating to the complaint and ensure that all parties involved are treated fairly.

#### 4- Resolution of the complaint

The person responsible for the complaint proposes appropriate solutions to resolve the complaint as quickly as possible.

Solutions may include corrective measures, or any other action required to resolve the complaint satisfactorily.

#### 5- Communication with the complainant

The person responsible for the complaint communicates regularly with the complainant to keep him/her informed of the progress of the investigation and the resolution of the complaint.

All communications must be professional, empathetic, and respectful.

#### 6- Closure of the complaint

Once the complaint has been resolved, the person responsible for the complaint must provide a written response to the complainant, summarizing the measures taken and the proposed solutions.

All information and documents relating to the complaint must be kept in a confidential file.