

Privacy Compliance Policy – Law 25

Table of contents

| | |
|--|---|
| 1. Scope | 3 |
| 2. Personal Information | 3 |
| 3. Privacy Officer (PO) | 3 |
| 4. Consent | 3 |
| 5. Collection and Processing of Personal Information | 3 |
| 6. Rights of Data Subjects | 4 |
| 7. Data Protection Risk Analysis | 4 |
| 8. Roles and Responsibilities | 5 |
| 9. Incidents | 5 |
| 10. Incident Log | 5 |
| 11. Notification to the Commission d'accès à l'information ("CAI") | 5 |
| 12. Accuracy of Personal Information | 5 |
| 13. Default Privacy Settings | 5 |
| 14. Automated Decision-Making..... | 6 |
| 15. Disclosure Without Consent | 6 |
| 16. Retention Period | 6 |
| 17. Use of Cookies and Tracking Technologies | 6 |
| 18. Informing Individuals About Technological Data Collection..... | 6 |
| 19. Portability of Computerized Personal Information..... | 6 |
| 20. Collection of Personal Information from Minors..... | 7 |
| 21. Cessation of Disclosure of Personal Information | 7 |
| 22. Method of Disclosure of Personal Information..... | 7 |
| 23. Response to Access and Correction Requests | 7 |
| 24. Training and Awareness | 7 |
| 25. Refusal to Provide Personal Information | 8 |
| 26. Policy Review..... | 8 |
| 27. Non-Compliance | 8 |



1. Scope

This Privacy Policy ("the Policy") applies to Alimplus Inc. and Groupe Mayrand Alimentation Inc. ("Groupe Mayrand"), as well as its divisions and subsidiaries, in accordance with Law 25 ("the Law") of the province of Quebec. The Policy applies to all employees, subcontractors, suppliers, and third parties who process personal information on behalf of Groupe Mayrand.

Groupe Mayrand is committed to respecting and protecting the privacy of users of its website, customers, suppliers, employees, and other individuals who interact with the company.

The Policy describes the personal information that is collected, how it is used, how it is disclosed to stakeholders, and the rights and choices available to individuals regarding their personal information.

2. Personal Information

This refers to any information that can be used to identify an individual. It is considered confidential and, except in specific circumstances, it cannot be disclosed without the consent of the individual concerned.

3. Privacy Officer (PO)

In accordance with the requirements of the Law, Groupe Mayrand has appointed a Privacy Officer ("PO") responsible for overseeing matters related to the protection of personal information. For any questions about this policy or to report an incident, an email can be sent to: renseignementspersonnels@mayrand.ca.

4. Consent

Consent is the voluntary and informed action by which an individual explicitly authorizes a business, website or app to collect, process and use their personal information.

The processes governing consent include:

- Obtaining valid and distinct consent for each specific purpose, using clear and straightforward language;
- Presenting the request for consent separately from other information if provided in writing;
- Providing all legally required information to individuals whose personal information is being collected;
- Informing individuals when a decision affecting them is made solely through automated processing;
- Informing individuals before using any technology that enables their identification, location tracking or profiling, and providing options to enable these features.

5. Collection and Processing of Personal Information

Groupe Mayrand has implemented the necessary processes to proactively manage consent (see Section 4) for the collection of personal information. Personal information is collected as follows:

- Directly from the individuals concerned;
- Through our service providers;
- Through cookies;
- Using tracking technologies.

Only the personal information necessary to provide products and services to the individuals concerned is collected. More specifically, only the personal data required for the purposes for which it was collected will be gathered and processed.

Clear and concise information will be provided to individuals about how their data will be used and their rights under the Law.

The following types of personal information may be collected:

- Name and contact details, which may include email, residential address and phone number. For online purchases, IP addresses and, in some cases, payment card information such as credit card number, expiration date and security code may be collected;
- Information related to credit applications, which, for sole proprietorships, may include name, address, phone number, email, banking details, and driver's license number.
- Employment-related information, such as name, address, email and any other information provided in résumés, during the hiring process and throughout the employee's tenure.

6. Rights of Data Subjects

Individuals have the right to:

- Request access to their personal data. Groupe Mayrand will respond to such requests within one month;
- Request the correction of inaccurate or incomplete personal data;
- Request the destruction of their personal data in circumstances where there is a risk of serious harm;
- Request that computerized personal information be provided in a clear and intelligible written format;
- Object to the processing of their personal data for certain purposes;
- Make requests and file complaints regarding the management of personal information;
- The portability of their electronic data (see Section 19).

7. Data Protection Risk Analysis

A data protection risk analysis process has been carried out to identify, assess and mitigate the risks associated with the processing of personal information. This process ensures compliance with the Law regarding data protection, safeguards sensitive information and protects individuals' privacy. Below is a step-by-step description of Groupe Mayrand's data protection risk assessment process:

- a. Scope of the data protection risk analysis
- b. Data inventory and mapping
- c. Identification of risks and threats
- d. Assessment of impact and likelihood
- e. Risk mitigation strategies
- f. Documentation and reporting

8. Roles and Responsibilities

All individuals involved in the protection of personal information understand their roles and responsibilities in this area. See Section 23 – Training.

9. Incidents

A personal information incident is a situation in which personal data is exposed or compromised without authorization. A major incident is one that poses a serious risk of harm.

A data privacy incident, also known as a data breach, occurs when there is unauthorized access to, disclosure of or loss of sensitive and confidential information. This may involve different types of data, including personal information, financial records, health data, intellectual property, etc.

A data privacy incident, also known as a data breach, occurs when there is:

- Unauthorized access to personal information, as defined by law;
- Unauthorized use of personal information, as defined by law;
- Unauthorized disclosure of personal information, as defined by law;
- Loss of personal information or any other breach of its protection.

10. Incident Log

In the event of a privacy incident, Groupe Mayrand maintains an incident log and promptly takes action to mitigate the risk of harm to affected individuals and to prevent similar incidents from occurring in the future.

11. Notification to the Commission d'accès à l'information ("CAI")

Groupe Mayrand has established a process for notifying the Commission d'accès à l'information (CAI) in the following cases:

- Any incident presenting a risk of serious harm (which is also communicated to the individuals concerned); and
- When identity verification involves the use of biometric characteristics or measurements.

12. Accuracy of Personal Information

The organization is committed to maintaining the accuracy and updating of individuals' personal information. If any inaccuracies are identified, corrections can be requested by email at: rh@mayrand.ca.

13. Default Privacy Settings

Employees' personal data is sent by email with a unique password. No other personal information is emailed to the organization's employees.

14. Automated Decision-Making

When decisions are made solely through automated processing of personal data, the company is committed to informing the individuals concerned of the use of such automation. Individuals have the right to contest these decisions and to request human intervention if necessary.

15. Disclosure Without Consent

The disclosure of personal information without the consent of individuals concerned is conducted in compliance with the Law;

- In the course of carrying out a mandate or fulfilling a service or business contract;
- Mayrand may disclose personal information about a deceased individual to their spouse or close relative if such information could assist the requester in their grieving process, provided that the deceased did not explicitly refuse to grant this right of access in writing.

16. Retention Period

Personal data is retained only for as long as necessary to fulfill the purposes for which it was collected. The retention period may vary depending on the type of data and needs of Groupe Mayrand.

Groupe Mayrand commits to destroying personal information once its intended purpose has been achieved or to anonymizing it for legitimate use, in accordance with the conditions and retention period set out by any applicable law.

17. Use of Cookies and Tracking Technologies

Cookies are used to collect information when individuals visit our website.

18. Informing Individuals About Technological Data Collection

When personal information is collected through technological means, individuals are informed via notices or pop-up windows on the organization's website.

19. Portability of Computerized Personal Information

Unless there are major practical obstacles, when personal information is collected through technological means directly from an individual, that individual may request that Groupe Mayrand provide the data in a structured, commonly used electronic format. This information may also be disclosed, upon request, to any person or organization authorized by law to collect it. When an individual exercises their right to data portability, they have the right to have the personal data transmitted directly from one data controller to another, where technically feasible.

Personal information that is collected and stored in paper format is excluded, as is any information created or inferred from personal data.

Requests for the portability of computerized personal information are processed by Groupe Mayrand within 30 days of receiving the request.

20. Collection of Personal Information from Minors

All personal information concerning minors under the age of 14 is collected only with the consent of the holder of parental authority or the legal guardian, except when the collection is for the benefit of the minor.

21. Cessation of Disclosure of Personal Information

Individuals concerned with specific personal information may request that Groupe Mayrand stop disclosing that information or have it de-indexed, including any hyperlinks associated with their name that provide access to the information through technological means. This applies when:

- The disclosure of the information violates the law or a court order;
- The disclosure of the information may cause serious harm to individuals' reputations or privacy rights (where the harm clearly outweighs the public's interest in the information or any person's interest in freedom of expression); and
- The requested cessation, re-indexing or de-indexing is limited to what is necessary to prevent further harm.

22. Method of Disclosure of Personal Information

Any third party to whom personal information is disclosed must comply with the following conditions under a prior agreement:

- Restricted access: Personal information may only be consulted by individuals who require it to perform their duties and who have signed a confidentiality agreement;
- Proper use: Personal information may only be used for the purpose specified in the detailed presentation of research activities.

Personal information may not be disclosed, published or shared in a way that enables the identification of the individuals concerned. No personal information collected from individuals will be disclosed to third parties, except in the following cases:

- To entities within Groupe Mayrand;
- To service providers who perform essential services for the company's operations, provided they need this personal information to fulfill their duties (service providers must comply with specific personal information protection requirements);
- To third parties when disclosure of personal information is required or authorized by law;
- Groupe Mayrand ensures that any transfer of personal data outside of Quebec complies with the requirements of Law 25.

23. Response to Access and Correction Requests

Access and correction requests are processed by Groupe Mayrand within 30 days of receipt.

24. Training and Awareness

It is important to train employees and other relevant stakeholders on best practices related to the requirements of Law 25. Training is provided at two levels:

- General training on Law 25 requirements for all Groupe Mayrand staff;
- More detailed training for staff members handling personal information.

25. Refusal to Provide Personal Information

Groupe Mayrand may refuse to disclose personal information concerning an individual when such disclosure is likely to reveal personal information about a third party or the existence of such information, and when this disclosure could seriously harm that third party, unless the third-party consents or it is an emergency situation endangering the life, health or safety of the individual concerned.

Under Section 40.1 of the Law, Groupe Mayrand must refuse to disclose personal information to an estate liquidator, a life insurance or death benefit beneficiary, an heir or a successor of the individual concerned, unless such disclosure would compromise the interests and rights of the requester in their capacity as liquidator, beneficiary, heir or successor.

26. Policy Review

This policy will be reviewed annually and updated as necessary to ensure ongoing compliance with Law 25.

27. Non-Compliance

Failure to comply with this policy may result in disciplinary action, including termination of employment or contract.