Aliments MLW Foods

Policy Framework for the Governance of the Management of Personal Information

Aliments MLW Foods

TABLE OF CONTENTS

1. **PREAMBLE** 1
2. **OBJECT** 1
3. **DEFINITIONS** 1
4. **SCOPE** 2
5. **HANDLING OF PERSONAL INFORMATION** 2
6. **PRIVACY IMPACT ASSESSMENT** 5
7. **RIGHTS OF DATA SUBJECTS** 5
8. **COMPLAINT HANDLING** 7
9. **SECURITY** 7
10. **CONFIDENTIALITY INCIDENTS** 7
11. **LOG OF CONFIDENTIALITY INCIDENTS** 7
12. **ROLES AND RESPONSIBILITIES** 8
13. **SANCTIONS** 9
14. **UPDATE** 9

1. PREAMBLE

As part of its activities and mission, MLW Foods Inc. ("the **Company**") processes personal information, including that of its consumers, visitors to its website, members of its staff, including its employees and job applicants. As such, it recognizes the importance of respecting privacy and protecting the personal information it holds, whether hosted internally or by a third party.

In order to meet its obligations in this regard, the Company has adopted this policy. It sets out the framework principles applicable to the protection of personal information held by the Company throughout its life cycle as well as the roles and responsibilities of stakeholders in the protection of personal information and the exercise of the rights of the individuals concerned.

The protection of personal information held by the Company is the responsibility of any individual who processes such information.

2. OBJECT

This policy:

- sets out the Company's governance principles with respect to personal information throughout its lifecycle;
- provides a framework for the exercise of individuals' rights;
- provides for the process for handling complaints relating to the protection of personal information;
- defines the Company's privacy roles and responsibilities.

3. DEFINITIONS

For the purposes of this policy, the following terms mean:

"**CAI**" means the Commission d'accès à l'information du Québec.

"**Life cycle**" refers to all the steps involved in the processing of personal information, i.e. the collection, use, disclosure, retention and destruction of the information, including payroll information.

"**Privacy Impact Assessment**" or "**PIA**" refers to the preventive approach that aims to better protect personal information and respect the privacy of individuals. This assessment consists of considering all the factors that may have positive or negative consequences on the privacy of the individuals concerned and implementing measures to mitigate the associated risks.

"**Privacy Incident**" refers to any unauthorized access, use or disclosure of personal information not authorized by law, or any loss or other breach of personal information.

"**Act**" refers to the *Act respecting the protection of personal information in the private sector* (PIPEDA) and any other legislation that may apply to the Company's personal information processing activities from time to time, such as *the Personal Information Protection and Electronic Documents Act* (PIPEDA).

"**Data subject**" refers to an individual to whom the personal information relates.

"**profiling**" refers to the collection and use of personal information to assess certain characteristics of an individual, including for the purposes of analyzing that individual's job performance, economic situation, health, personal preferences, interests, or behaviour

"**Personal Information**" means any information about an individual that allows that person to be identified directly – either by the use of that information alone – or indirectly – or by combination with other information.

"**Sensitive Personal Information**" refers to any personal information that – by its nature, including medical, biometric or otherwise sensitive information, or by the manner in which it is used or disclosed – gives rise to a high degree of reasonable expectation of privacy.

"**Privacy Officer**" refers to the person within the Company who is responsible for ensuring compliance with and enforcement of the Privacy Act.

4. SCOPE

This policy applies to personal information held by the Company and to any individual who processes personal information on behalf of the Company.

5. HANDLING OF PERSONAL INFORMATION

Personal information is protected throughout its life cycle in accordance with the following principles, except as provided by law.

5.1. Collection

5.1.1. The Company collects only the personal information necessary to carry out its activities. Before collecting personal information, the Company determines the purposes for which it is processed, which must be serious and legitimate.

5.1.2. Personal information is collected from the individual concerned unless the law permits the collection of personal information from a third party.

5.1.3. At the time of collection, and thereafter upon request, the Company informs the individuals concerned, at a minimum of:

- the purposes for which the information is collected;
- the means by which the information is collected;
- the rights of access and rectification provided for by law;
- the right to withdraw consent to the disclosure or use of the information collected;
- where applicable, the name of the third party for whom the collection is made;
- where applicable, the names of the third parties or categories of third parties to whom the

information must be disclosed for the declared purposes;

- where applicable, the possibility that the information may be communicated outside Québec;
- where applicable, the use of a technology including functions that allow it to be identified or profiled therein.
- the means offered to activate the functions to identify, locate or carry out profiling.

5.1.4. The information listed in the 5.1.3 is given in simple and clear terms, through a privacy policy or a "just-in-time" notice».

5.1.5. The individual who provides his or her personal information after receiving the information in paragraph 5.1.3 is deemed to consent to the use and disclosure for the stated purpose.

5.1.6. At the request of an individual, the Company must also inform them of the following:

- personal information collected from the employee;
- the categories of individuals who have access to such information within the Company;
- retention period of this information;
- the Company's Privacy Officer contact information.

5.1.7. Where consent is required by law, it must be explicit, free, informed and given for a specific purpose. It is requested for each of these purposes, in simple and clear terms. This consent is valid only for the time necessary to achieve the purposes for which it was requested.

5.2. Usage

5.2.1. The Company uses personal information only for the purposes for which the information was collected. However, the Company may change these purposes if the individual concerned consents to the change beforehand.

5.2.2. The Company may also use personal information for secondary 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 (compatible purposes exclude commercial or philanthropic prospecting);
- when the use is clearly for the benefit of the individual.
- when its use is necessary for the purposes of fraud prevention and detection or to evaluate and improve protection and security measures.
- where its use is necessary for the purpose of providing or delivering a product or service requested by the data subject.
- where the use is necessary for study, research or statistical purposes and the information is de-identified.

5.3. Communication

5.3.1. Subject to exceptions provided by law, the Company may not disclose personal information without obtaining the consent of the individual concerned. Consent must be given specifically when sensitive personal information is involved.

5.3.2. The Company may disclose personal information without consent to a representative or service provider as part of a mandate or service contract, including a technological tool hosted on a cloud computing platform. For this purpose, the Company must enter into a written agreement with the representative or service provider, which stipulates, at a minimum, the actions that the representative or service provider must take:

- to ensure the protection of the confidentiality of the personal information disclosed;
- to ensure this information is used only in the exercise of the mandate or the execution of the contract;
- to ensure it is not retained after the mandate or contract expires.

In addition, the agreement must indicate the following:

- the representative or service provider must promptly notify the Company Privacy Officer of any breach or attempted breach by any person of any of the obligations relating to the confidentiality of the information disclosed;
- The Company's Privacy Officer reserves the right to conduct any verification relating to this confidentiality.

5.4. Conservation

5.4.1. The Company takes all reasonable steps to ensure that the personal information under its control is up-to-date, accurate and complete for the purposes for which it is collected or used.

5.4.2. The Company retains personal information for as long as necessary to conduct its business, subject to applicable retention periods or legal requirements.

5.5. Destruction and anonymisation

5.5.1. When the purposes for which the personal information collected is fulfilled, the information is destroyed or anonymized, according to the Company's retention periods.

6. PRIVACY IMPACT ASSESSMENT

6.1. The Company conducts a Privacy Impact Assessment in the following contexts, among others:

- before initiating a project involving the acquisition, development, or overhaul of an information system or electronic service delivery that involves personal information;
- when it intends to disclose personal information outside Québec.

6.2. In conducting a Privacy Impact Assessment, the Company considers the sensitivity of the information to be processed, the purposes for which it is used, the amount, distribution and format, and the proportionality of the measures proposed to protect the personal information.

6.3. In addition, when personal information is disclosed outside Québec, the Company ensures that it receives adequate protection, particularly with regard to generally recognized principles of personal information protection.

6.4. The purpose of conducting a Privacy Impact Assessment is to demonstrate that the Company has complied with all obligations related to the protection of personal information and that all necessary measures have been taken to effectively safeguard such information.

7. RIGHTS OF DATA SUBJECTS

7.1. Subject to the provisions of the law, any data subject about whom the Company holds personal information has the following rights:

- the right to access and obtain a copy of personal information held by the Company, whether in electronic or non-electronic format;
    - Unless it raises serious practical difficulties, computerized personal information collected from the individual and not created or inferred from personal information about that person, shall be disclosed in a structured and commonly used technological format, at the request of the individual. The information shall also be disclosed, upon request, to any person or body authorized by law to collect such information.
- the right to request rectification of any incomplete or inaccurate personal information held by the Company.
- the right to request the deletion of outdated or unsubstantiated information, or to provide written comments to the Company's Privacy Officer;
- the right to request that the Company cease disseminating information or to de-index any hyperlink associated with their name by technological means, when the dissemination of such information violates the law or a court order;
- the right to request that the Company cease disseminating information or to de-index or re-index any hyperlink associated to their named, when the following conditions are met:
    - the dissemination of this information causes them serious prejudice relating to the right to respect for their reputation or private life;

- this harm is manifestly greater than the public's interest in knowing this information or the interest of any person in expressing themselves freely;
- the cessation of dissemination, re-indexing or de-indexation requested does not go beyond what is necessary to prevent the harm from being perpetuated, taking into account, in particular, whether or not the person concerned is a public figure, whether the information concerns a minor, whether the information is up-to-date and accurate, the sensitivity of the intelligence, the context in which the intelligence is disseminated, the time elapsed between the dissemination of the intelligence and the request made to the Society;

7.2. While the right of access can be exercised at any time, access to documents containing this information is subject to certain exceptions identified by law.

7.2.1. The Company may refuse to disclose personal information about him or her to an individual where disclosure of the information is likely to:

- hinder an investigation carried out by its internal security service for the purpose of preventing, detecting or punishing crime or offences against the law or, on its behalf, by an external service with the same purpose or by a holder of a security agency or investigation agency licence issued in accordance with *the Private Security Act;*
- affect a legal proceeding in which any of these parties has an interest.

7.2.2. the Company must refuse to disclose personal information to an individual:

- to an individual where disclosure would likely reveal personal information about a third party or the existence of such information and such disclosure would be likely to cause serious harm to that third party, unless the third-party consents to its disclosure or it is an emergency endangering the life, health or security of the person concerned;
- to the liquidator of the estate, the beneficiary of a life insurance policy or death benefit, the heir or successor of the person to whom the information relates, unless such disclosure would jeopardise the interests and rights of the person requesting it as liquidator, beneficiary, heir or successor, all subject to the right of the spouse or parent of a deceased person mentioned above.

7.3. The request for access to personal information must be specific enough to allow the Privacy Officer to identify the personal information. The right of access applies only to existing personal information.

7.4. The Privacy Officer responds in writing to requests for access or correction, in a timely manner and no later than 30 days after the date of receipt of the request.

7.5. Access to the personal information contained in a file is free of charge. However, the Company may charge a reasonable fee for the transcription, reproduction or transmission of such information, after informing the applicant of the approximate amount payable, prior to proceeding with the transcription, reproduction or transmission of such information.

7.6. Where the Privacy Officer agrees to a request for rectification or deletion, they shall notify any person who has received the information within the previous six months and, if applicable, the

person who holds the information. In addition, the Privacy Officer will issue to the requester, free of charge, a copy of any personal information that has been amended or added or, as the case may be, an attestation of the personal information deleted.

7.7. If the Company fails to respond within 30 days of receipt of the request, it will be deemed to have refused to comply with it. That said, the Privacy Officer must give reasons for any refusal to grant a request and indicate the provision of the statute on which the refusal is based, the remedies available to the requester under the law, and the time within which they may be exercised. The Privacy Officer must also provide assistance to the requester upon request to help them understand the refusal.

8. COMPLAINT HANDLING

Any complaint regarding the Company's privacy practices or its compliance with legal requirements regarding personal information will be forwarded to the Privacy Officer, who will respond within 30 days.

You may direct any request, question, complaint or comment regarding this policy to our Privacy Officer at dataprivacy@mlwfoods.com.

9. SECURITY

9.1. The Company implements reasonable security measures to ensure the confidentiality, integrity and availability of personal information collected, used, disclosed, retained or destroyed. These measures take into account, among other things, the degree of sensitivity of the personal information, the purpose for which it was collected, its quantity, its location and its medium.

9.2. The Company manages the access rights of its employees so that only those who need access to personal information as part of their duties can access it.

10. CONFIDENTIALITY INCIDENTS

10.1. Any privacy incidents involving personal information must be reported to the Privacy Officer. The Company then takes reasonable measures to reduce the risk of harm being and to prevent future incidents from occurring in the future.

10.2. Any privacy incidents are recorded in the privacy incident log, regardless of the severity.

10.3. If the privacy incident poses a risk of serious harm to the individuals concerned, the Company will promptly notify them and the *Commission d'accès à l'information du Québec,* after consulting a lawyer.

11. LOG OF CONFIDENTIALITY INCIDENTS

11.1. In accordance with the law, the Company maintains a record of privacy incidents.

11.2. The Privacy Officer is responsible for maintaining the register, retaining for the time required by law (five years for Quebec) and updating it.

12. ROLES AND RESPONSIBILITIES

12.1. The protection of the personal information held by the Company is based on the commitment of all those who handle this information, and in particular the following:

12.2. This includes, but is not limited to, the person responsible for the protection of personal information, members of the executive team, the IT support team, Human Resources, Finance and all other personnel who collect, process, or manage personal information.

- ensures compliance with and implementation of the law.
- ensures the establishment and implementation of policies and practices governing the governance of the company with respect to personal information and ensuring the protection of this information, in particular by approving such information.
- is consulted, for the purposes of a Privacy Impact Assessment, at the outset of any project involving the acquisition, development and redesign of an information system or electronic service delivery involving the collection, use, disclosure, retention or destruction of personal information
- at any stage of a project mentioned above, the Privacy Officer may suggest measures to ensure the protection of the personal information involved in the project, such as:
    - the appointment of a person responsible for the implementation of the protection measures;
    - the protection of personal information in any project documents;
    - a description of the responsibilities of the project participants in relation to the protection of personal information;
    - conducting training activities on the protection of personal information for project participants
- The person responsible for the protection of personal information is responsible for maintaining the privacy Incident Log.
- participates in the assessment of the risk of serious harm related to a privacy incident, in particular with regard to the sensitivity of the information concerned, the anticipated consequences of its use and the likelihood that this information will be used for malicious purposes;
- where applicable, records the disclosure of a privacy incident to a person or body that may reduce a risk of harm;
- where applicable, conducts audits of confidentiality obligations related to the disclosure of personal information in the context of mandates or service contracts entrusted to third parties in accordance with section 5.3.2 of this policy.
- receives written requests to exercise rights from data subjects and ensures compliance with section 7 of this policy.

12.3. The senior management:

- approves this policy and other documents forming the governance framework, as well as any amendments to them.
- receives and reviews the report of the Privacy Officer.
- keeps abreast of the Company's privacy activities and makes the actions it deems appropriate to maintain an acceptable level of risk for the Company.

12.4. Any individual, including any service provider, who handles personal information held by the Company:

- acts with caution and incorporates the principles set out in this policy into its activities;
- only access information necessary for the performance of his duties;
- integrates and retains personal information only in files intended for the performance of its functions;
- stores these records in such a way that only authorized persons have access to them;
- protects access to personal information in its possession or to which it has access by means of a password;
- refrains from disclosing personal information that comes to knowledge in the course of his or her duties, unless duly authorized to do so;
- refrains from retaining, at the end of his employment or contract, personal information obtained or collected in the course of his duties and continues to uphold confidentiality obligations;
- destroys any personal information in accordance with the Company's retention periods;
- participates in privacy awareness and training activities on personal information protection intended for them;
- reports any breach, privacy incident or any other situation or irregularity that could compromise in any way the security, integrity or confidentiality of personal information in accordance with the procedure established by the Company.

13. SANCTIONS

Any person who violates this policy is liable to disciplinary or contractual sanctions, which may extend to the termination of the employment or business relationship.

14. UPDATE

In order to keep up with changes in applicable privacy laws and the Company’s practices, this policy may be updated.

Effective Date: August 2025.