GROUPE GRANDIO

Groupe Grandio

Personal Data Protection Framework Policy

Personal Data Protection Program

Last Revision Date: May 13, 2025

TABLE OF CONTENTS

1. PREAMBLE

In the course of their activities, Groupe Grandio (13401537 Canada Inc., hereinafter the "**Parent Company**"), its subsidiaries, affiliated companies, and groups of companies (collectively, "**Grandio**") process personal data, including that of their restaurants' guests, visitors to their websites and apps, loyalty program members, employees, as well as directors and executives. As such, Grandio understands the importance of respecting privacy and protecting the personal data it holds.

To fulfill its obligations under *Québec's Private Sector Privacy Act*, Grandio has adopted the following policy. It outlines the guiding principles applicable to the protection of personal data throughout its lifecycle, the rights of individuals, and the roles of stakeholders in implementing the law at Grandio.

This policy completes the Data Security and Cybersecurity Policy regarding the protection of personal data.

2. PURPOSE

This policy:

- Outlines the Documentary Framework that applies to personal data held by Grandio;
- Establishes Grandio's principles and governance rules regarding personal data throughout its lifecycle;
- Defines the roles and responsibilities of stakeholders in protecting personal data;
- Describes the training and awareness-raising activities Grandio provides to its personnel.

3. SCOPE

This policy applies to personal information collected or held by the Parent Company and any affiliated company or group of companies that holds personal data in the frame of its activities. It applies to any person processing personal data on behalf of these companies. When the Parent Company acquires a new company, the latter must implement the personal data protection program no later than six months following the completion of the transaction, with support from the Privacy Protection Committee, if required.

The Parent Company, affiliated companies, and groups of companies include, but are not limited to:

- 13401537 Canada Inc.
- Groupe Sportscene Inc. and 13668843 Canada Inc. (La Cage – Brasserie Sportive restaurants)
- Le Groupe Bistronomie Inc.
- Restaurants Chez Lionel (Québec) Inc. (Chez Lionel – Brasserie Française restaurants)

- Restaurants IRU (Québec) Inc. (IRU Izakaya – Japanese Brasserie restaurants)
- Le Groupe Restos Plaisirs Inc. (including Cochon Dingue, Ciel!, Lapin Sauté, Paris Grill, and Café du Monde restaurants)
- 121657245 Canada Inc. (Moishes restaurant)
- 14707923 Canada Inc. (Gibbys restaurant)
- Niji Sushi Bar et Restaurant Inc. (Niji Sushi restaurants)
- 16096018 Canada Inc. (Il Teatro – Italian Brasserie restaurants)
- 15679249 Canada Inc. (Brasseurs du Monde restaurants)
- Brasseurs du Monde Inc. (microbrewery)
- 9246-9394 Québec Inc. (La Cage – Event Catering)

  This list is not exhaustive.

Compliance with this policy is mandatory, and Grandio is committed to upholding it.

Any request for an exemption from this policy must be duly justified and submitted to the Privacy Officer for approval, and communicated to the Board of Directors of the Parent Company by the Privacy Officer. A request for an exemption is submitted and processed in accordance with Grandio's documentary framework, where applicable.

4. DOCUMENTARY FRAMEWORK

This policy is the foundational document for Grandio's compliance program for personal data protection, from which other policies, guidelines, procedures, or documents may derive, covering topics such as:

- Procedures for handling and processing exemption requests;
- Obtaining valid consent;
- Conducting privacy impact assessments;
- Communication between Grandio entities;
- Disclosure to third parties without consent;
- Disclosure of personal information outside Quebec;
- Exercise of individuals' rights;
- Retention, archiving, or destruction;
- Handling of individual complaints.

Grandio's compliance program is based on a documentary framework defined as follows:

- Framework Policy: Outlines Grandio's guiding principles for personal data protection and the approval mechanism for documents forming Grandio's documentary framework.

- Internal Policy or Directive: Documents the guiding principles, requirements, and expectations concerning a specific topic, i.e., “what to do.”
- Procedure, Guide, or Process: Provide a detailed sequence of steps or actions required to implement internal policies or directives, i.e., “how to do it”.

5. DEFINITIONS

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

“**Just-in-time notice**”: The transparency notice provided to an individual when their personal data is requested.

“**Documentary Framework**”: The set of legal governance documents adopted under this policy to implement Grandio’s personal data protection program.

“**CAI**”: The Commission d’accès à l’information du Québec.

“**Privacy Protection Committee**”: The committee established by the Parent Company to ensure compliance with and implementation of personal data protection laws.

“**Professional contact details**”: Personal data relating to the performance of a role within a company, such as name, title, position, and the postal address, email address, and telephone number of the workplace.

“**Life**”: The set of stages involved in processing personal data, including collection, use, disclosure, retention, and destruction.

“**Privacy Impact Assessment (PIA)**”: The process aimed at protecting personal data and respecting personal privacy. It is a form of impact analysis, evolves over time, and must be reviewed throughout the project.

“**Privacy incident**”: Any unauthorized access, use, or disclosure of personal data under the law, or any loss or other breach of its protection.

“**Law**”: The *Private Sector Privacy Act* (Quebec) and any regulations arising from it.

“**Data Subject**”: A natural person to whom the personal data relates.

“**President and Chief Executive Officer of the Parent Company**”: The person with the highest authority within the parent company.

“P**rofiling**”: The collection and use of personal data to assess an individual’s characteristics, especially for analyzing work performance, economic situation, health, personal preferences, interests, or behavior.

“P**ersonal data**”: Any data relating to an individual that allows them to be identified directly through that data alone or indirectly by combining it with other data.

“**Publicly available personal data**”: Personal data declared public by any applicable law.

"**Sensitive personal data**": Personal data which, due to its nature (e.g., medical, biometric, or otherwise personal) or the manner in which it is used or disclosed, gives rise to a high reasonable expectation of privacy.

"**Privacy Officer**": The person in the Parent Company and each of its subsidiaries and affiliated companies who ensures compliance with and the implementation of personal data protection laws.

6. GUIDING PRINCIPLES

Personal data is protected throughout its lifecycle in accordance with the following principles, except as provided for by law. Professional contact details and publicly available personal data are not subject to these guiding principles.

6.1. Collection

6.1.1. Grandio collects only the personal data required for its activities. Before collecting personal data, Grandio determines the purposes of its processing.

6.1.2. At the time of collection, and subsequently upon request, Grandio informs individuals of the mandatory content required by law, including the purposes of collection, the use of technologies enabling profiling (if applicable), and the right to withdraw consent to the use or disclosure of personal data by Grandio.

6.1.3. The information referred to in paragraph 6.1.2 is provided in clear and simple terms through a privacy policy or a just-in-time notice.

6.1.4. An individual who provides their personal data after receiving the information in paragraph 6.1.2 is presumed to consent to its use and disclosure for the stated purposes.

6.2. Use

6.2.1. Grandio uses personal data only for the purposes for which it was collected. However, Grandio may modify these purposes with the individual's prior consent.

6.2.2. It may also use the data for other purposes without the individual's consent in cases permitted by law.

6.3. Disclosure

6.3.1. Subject to exceptions provided for by law, Grandio may not disclose any personal data without the individual's consent.

6.3.2. When personal data is disclosed outside Quebec, Grandio conducts a Privacy Impact Assessment (PIA) in accordance with section 7 of this policy.

6.3.3. Grandio maintains a register of any disclosures of personal data without consent. The register records disclosures required by law, including:

- To a person or organization with the authority to compel Grandio to disclose personal data and who requests it in the course of their duties (e.g., a police officer with a warrant requesting personal data about an employee suspected of fraud);
- To a person to whom disclosure is required due to an emergency endangering the individual's life, health, or safety;
- To a person or organization for the purposes of a mandate or service or business contract (e.g., a payroll service provider);
- To the other party in a business transaction, if the disclosure is necessary to conclude the transaction (e.g., Grandio sells a subsidiary and must disclose personal data for this purpose);
- To a person who may use it for study, research, or statistical purposes;
- To a person authorized by law to collect debts on behalf of others and who requires it for that purpose in the course of their duties;
- To a person if the information is required to collect a debt owed to Grandio.

6.4. **Retention**

6.4.1. Grandio takes all reasonable measures to ensure that the personal data it holds is up-to-date, accurate, and complete for the purposes for which it is collected or used.

6.4.2. Grandio retains personal data for as long as required to fulfill the purposes for which it was collected, subject to any applicable retention obligations, in accordance with Grandio's retention schedule.

6.5. **Destruction or Anonymization**

6.5.1. When the purposes for which the personal data was collected are achieved, the information is destroyed or, in some cases, anonymized in accordance with Grandio's retention schedule and, where applicable, Grandio's documentary framework.

7. PRIVACY IMPACT ASSESSMENTS

7.1. Conducting a Privacy Impact Assessment (PIA) is a process that helps demonstrate that Grandio has met all its obligations regarding the protection of personal data and that all appropriate measures have been taken to effectively protect such data.

7.2. Grandio conducts a PIA, particularly in the following cases:

- Before undertaking a project to acquire, develop, or redesign an information system or electronic services product involving personal data;

- Before disclosing personal data without the consent of individuals to a person or organization wishing to use it for study, research, or statistical purposes;
- Before disclosing personal data outside Quebec.

7.3. When conducting a PIA, Grandio considers the sensitivity of the information to be processed, the purposes of its use, its quantity, distribution, and medium (or storage medium), as well as the proportionality of the measures proposed to protect personal data. Grandio also considers the criteria established by law for each PIA.

7.4. All PIAs are conducted in accordance with Grandio's documentary framework.

8. RIGHTS OF DATA SUBJECTS

8.1. At the request of a data subject, Grandio must inform them of:

- The personal data collected from them;
- The categories of persons within Grandio who have access to this data;
- The retention period for this data;
- The contact details of Grandio's Privacy Officer.

8.2. To the extent provided by law, any data subject about whom Grandio holds personal data has the following rights:

- The right to withdraw consent to the use and disclosure of personal data collected by Grandio;
- The right to access personal data held by Grandio and obtain a copy in an electronic or other format;
- Unless it poses significant practical difficulties, at the request of a data subject, Grandio shall communicate computerized personal data collected from them in a structured, commonly used technological format;
- The right to have incomplete or inaccurate personal data held by Grandio rectified;
- The right to request the deletion of data in certain circumstances or to submit written comments to Grandio;
- The right to be informed, where applicable, that personal data is used to make a decision based on fully automated processing;
- The right to request that Grandio cease disseminating data or de-index any hyperlink associated with their name, under certain conditions.

8.3. The Privacy Officer shall respond in writing to requests to exercise the rights outlined in paragraph 8.1 promptly and, in any case, no later than 30 days from the date of receipt of the request.

8.4. Any request to exercise rights is handled in accordance with Grandio's documentary framework.

9. PERSONAL DATA SECURITY

9.1. Grandio implements reasonable security measures to ensure the confidentiality, integrity, and availability of personal data collected, used, disclosed, retained, or destroyed. These measures take into account the sensitivity of the data, the purpose of its collection, and its quantity, location, and medium.

9.2. Grandio manages its personnel's access rights to ensure that only personnel subject to a confidentiality agreement (where applicable) and requiring access to it to perform their duties have access to personal data.

10. PRIVACY INCIDENT

10.1. Any privacy incident is handled in accordance with Grandio's documentary framework.

10.2. In accordance with the law, Grandio maintains a privacy incident register.

10.3. If a privacy incident poses a risk of serious harm to individuals, Grandio promptly notifies them and the CAI.

10.4. The register is maintained for five years following the date of the last incident or the end of the period of the last incident.

11. TRAINING AND AWARENESS-RAISING ACTIVITIES

11.1. Grandio provides training and awareness-raising activities to its personnel regarding personal data protection.

11.2. Failure to complete the required training and awareness-raising activities violates Grandio's documentary framework, and individuals may face sanctions depending on the nature and severity of the violation.

12. ROLES AND RESPONSIBILITIES

12.1. The protection of personal data held by Grandio relies on the commitment of all those who process such data, particularly the following stakeholders:

12.2. President and Chief Executive Officer:

- Ensures compliance with the law and its implementation;
- Ensures that the Privacy Officer is provided with adequate resources to fulfill their mandate and implement Grandio's personal data protection program.

12.3. Board of Directors of the Parent Company:

- Approves this policy and any significant amendments thereto, based on the Privacy Officer's recommendation;
- Receives and reviews the Privacy Officer's report;
- Is informed of Grandio's personal data protection activities and takes appropriate actions to maintain an acceptable level of risk for Grandio.

12.4. Privacy Protection Committee:

- Approves this policy and all documents forming Grandio's documentary framework, as well as any significant amendments, based on the Privacy Officer's recommendation;
- Receives and reviews any issues related to personal data protection submitted by the Privacy Officer.

12.5. Privacy Officer:

- Ensures compliance with the law and its implementation across Grandio;
- Is responsible for the application and implementation of this policy and other documents forming Grandio's documentary framework;
- Designs Grandio's documentary framework and makes appropriate updates;
- Recommends to the Board of Directors of the Parent Company any documents related to the personal data protection program or any issues deemed appropriate;
- Supports the Parent Company's teams, as well as affiliated companies and groups, in implementing the program, including acting as a point of contact for associated questions;
- Where necessary, produces a report on activities related to Grandio's personal data protection program and submits it to the Board of Directors of the Parent Company as part of the quarterly risk management report;
- Oversees the coordination of the Privacy Protection Committee's response to a privacy incident and the maintenance of the privacy incident register;
- Receives and processes data subjects' rights requests and ensures that responses comply with Grandio's documentary framework;
- Is consulted from the outset of Privacy Impact Assessments (PIAs) and may suggest measures to mitigate personal data protection risks.

12.6. Any person processing personal data on behalf of Grandio:

- Acts with caution and integrates the principles and guidelines set out in the documentary framework into their activities;
- When collecting personal data from individuals, ensures consent is obtained in accordance with the law and documented as per the documentary framework;
- Accesses only the data required to perform their duties;
- Stores records in a manner that restricts access to authorized persons only;
- Must refrain from disclosing personal data obtained in the course of their duties unless duly authorized;
- Must not retain personal data after the end of their employment or contract and must comply with their confidentiality obligations;
- Retains and destroys personal data in accordance with Grandio's documentary framework;
- Participates in personal data protection awareness-raising and training activities intended for them;
- Identifies situations requiring a PIA and completes the appropriate documentary framework documents;
- Immediately reports any breach, privacy incident, or other situation or irregularity that could compromise the security, integrity, or confidentiality of personal data to the Privacy Officer;
- Immediately reports any request to exercise rights or complaints regarding Grandio's personal data protection practices to the Privacy Officer.

13. COMPLAINT MANAGEMENT

Any complaint regarding Grandio's personal data protection practices or compliance with legal requirements concerning personal data is forwarded to the Privacy Officer, who shall respond within thirty (30) days.

14. SANCTIONS

Compliance with this policy and all other documents forming the governance framework is mandatory across Grandio. Personnel who fail to comply may face disciplinary measures ranging from a disciplinary notice to termination or, for consultants, contractual sanctions and penalties, which may include, among other things, contract termination and claims for damages. Additional training and awareness-raising may also be provided in cases of non-compliance.

15. REVIEW

To keep pace with changes in applicable personal data protection laws and to improve Grandio's personal data protection program, this policy may be updated as needed, at least every three years.

16. RESPONSIBILITY

This policy is the responsibility of the Privacy Officer.

17. ENTRY INTO FORCE

This policy comes into force upon its adoption by the Board of Directors of the Parent Company, based on the Privacy Officer's recommendation.

Revision History

Version	Author	Comments	Date

Effective Date: March 28, 2024.