EVOVEST

# Privacy Policy

The Firm and its employees must protect the privacy of clients' personal information, ensuring its confidentiality and security. The collection, use, retention, disclosure, and destruction of personal information must be done in accordance with Quebec's Law 25, which amends the Act Respecting the Protection of Personal Information in the Private Sector. Any disclosure must comply with legal and regulatory requirements, including provisions for consent, legal obligations, or legitimate interest.

The Firm has established a "***Privacy Policy for the Collection, Use, Retention, and Destruction of Personal Information***," which is provided to clients during the account opening process or with the investment policy statement. The Chief Privacy Officer (CPO) is responsible for ensuring that all employees and agents are familiar with the Firm's privacy policies before interacting with clients, and that all roles and responsibilities throughout the lifecycle of personal information are clearly defined and communicated.

## ROLES AND RESPONSIBILITIES

Throughout the lifecycle of personal information, all employees are responsible for its protection:

- **Collection:** Employees must ensure that personal information is collected lawfully and only for the purposes clearly identified to the client.
- **Use:** Information may only be used for its intended purpose and must be handled with strict confidentiality.
- **Retention:** Personal information should be retained only as long as necessary to fulfill the purposes for which it was collected, unless otherwise required by law.
- **Destruction:** Once the retention period expires, personal information must be securely destroyed, ensuring that no unauthorized individuals can access the data. The destruction process will follow secure procedures, such as document shredding or digital data deletion, in compliance with Law 25.

The CPO will oversee this process and ensure compliance at each stage of the information lifecycle.

## TRAINING PROGRAM

1. **New Employees or Agents:**

Before dealing with clients, new employees or agents must review the policy. A meeting will be held between the CPO and the employee to clarify any questions. The employee must then sign the Employee's Certificate in the compliance system, acknowledging their understanding of the Firm's privacy obligations, including the retention and destruction of personal data.

2. **Existing Employees or Agents:**

On an annual basis, or as required, every employee or agent must review the policy meeting with the CPO will follow to ensure comprehension, and the employee will acknowledge this by signing the Employee's Certificate in the compliance system.

The CPO will ensure that the Firm's privacy policy is followed by periodically verifying that it is prominently displayed, implemented, and accessible. Concerns or complaints regarding personal information handling must be directed to the CPO, and the Firm will investigate and resolve any complaints through a well-documented complaint management process.

## COMPLAINT MANAGEMENT PROCESS

To ensure compliance with Law 25 and address concerns about the handling of personal information, the Firm has established a formal process for handling privacy-related complaints:

- **Filing a Complaint:** Clients or employees can file a privacy-related complaint by contacting the CPO.
- **Investigation:** Upon receipt of a complaint, the CPO will conduct a thorough investigation to determine whether there has been a breach or mishandling of personal information. The Firm's designated officer is responsible for responding to any client requests for access to or rectification of personal information within 30 days of receiving the request. If more time is needed, the client or employee will be notified in writing of the extension, as allowed by applicable laws.
- **Resolution:** The Firm will take corrective action where necessary and communicate the resolution to the complainant.
- **Reporting:** If required by law, the CPO will notify the Commission d'accès à l'information (CAI) and other relevant authorities in Quebec of any significant breach.

## PROTECTION OF PERSONAL INFORMATION

As part of the Firm's operations, personal information such as identity (e.g., name, date of birth, citizenship), financial details (e.g., income, marital status), and other relevant data (e.g., social insurance number) may be collected. This information is confidential, and employees must safeguard it in compliance with Quebec's Law 25. Personal information can only be disclosed with the client's explicit written consent or legal authorization.

Employees must ensure that personal information is used only for its intended purposes, such as opening accounts, fulfilling regulatory obligations, or enforcing the Firm's legal rights. Unauthorized access, use, or disclosure of personal information is strictly prohibited.

## CLIENTS' ACCESS TO PERSONAL INFORMATION

Clients have the right to access their personal information and request corrections if necessary. However, access may be restricted in cases permitted by law. Clients may request access or inquire about the Firm's privacy policies by contacting the CPO.

## BASIC RULES FOR PROTECTING CONFIDENTIALITY

1. **Limit Disclosure:**

Confidential information must only be shared with individuals or entities with a legitimate need-to-know or with the client's explicit consent, in compliance with legal obligations under Law 25.

2. **Prevent Unauthorized Access:**

Employees must take all necessary precautions to safeguard confidential information, including:

- Avoiding discussions of confidential information in public or unsecured locations.
- Restricting access to computer files with appropriate security measures.
- Ensuring that no unauthorized persons, including temporary staff, gain access to confidential data without proper authorization.

3. **Document Disposal:**

Any unnecessary copies of documents containing confidential information must be securely shredded or destroyed.

## EMPLOYEES' ONGOING TRAINING ON PRIVACY PROTECTION

Employees will receive regular training on privacy protection and the importance of complying with Law 25. The training will cover all aspects of the information lifecycle, including collection, use, retention, and secure destruction of personal information.

## PRIVACY BREACH MANAGEMENT

A privacy breach occurs when there is unauthorized access, collection, or disclosure of personal information. Any breach must be reported immediately. The CPO will lead investigations and ensure corrective actions are taken, in accordance with legal obligations under Law 25, including the notification of affected individuals and the Commission d'accès à l'information (CAI).

**Incident Response Plan:**

- **Containment:** Immediately contain the breach.
- **Investigation:** The CPO will lead the investigation and escalate internally or externally as necessary.
- **Risk Assessment:** Determine the scope of the breach, including the type of information involved and the number of individuals affected.
- **Notification:** If required, notify affected individuals, regulatory bodies, and other relevant authorities such as the CAI.
- **Future Prevention:** Take necessary steps to prevent future breaches, such as updating policies, enhancing security, or providing additional training.

## Disclosure to External Suppliers and Authorities

Evovest may need to share personal information with external suppliers to provide services or manage business or employment relationships. Before doing so, Evovest ensures that these suppliers have adequate measures in place to maintain confidentiality and security, and that they use the information only for its intended purposes.

In certain cases, Evovest may be legally required to disclose personal information to government authorities, regulatory bodies, or self-regulatory organizations. Some external suppliers may use data processing technologies located outside of Quebec or Canada, which could subject the information to the laws and courts of those jurisdictions.

## TEN PRIVACY PRINCIPLES

In accordance with Law 25 and the Act Respecting the Protection of Personal Information in the Private Sector, the Firm adheres to the following principles:

1. **Accountability:** The Firm is responsible for personal information under its control and must ensure third parties comply with privacy regulations.
2. **Identifying Purposes:** The purposes for collecting personal information must be clearly communicated to clients before collection.
3. **Consent:** Personal information cannot be collected, used, or disclosed without the client's knowledge and consent, except in cases permitted by law.
4. **Limiting Collection:** Only personal information necessary for identified purposes should be collected, using lawful means.

5. **Limiting Use, Disclosure, and Retention:** Personal information may only be used or disclosed for its original purposes or with further consent. It must be retained only as long as necessary and securely destroyed after.
6. **Accuracy:** Personal information must be accurate, complete, and up to date.
7. **Safeguards:** The Firm must protect personal information with appropriate security measures.
8. **Openness:** The Firm must be transparent about its policies and procedures for protecting personal information.
9. **Individual Access:** Clients have the right to access their personal information and request corrections.
10. **Challenging Compliance:** Clients may challenge the Firm's compliance with these principles through the CPO or relevant authorities.

## Privacy Impact Assessments (PIA)

In compliance with Quebec's Law 25 and following the guidelines from the Commission d'accès à l'information du Québec (CAI), the Firm commits to conducting **Privacy Impact Assessments (Évaluation des facteurs relatifs à la vie privée, EFVP)** under the following conditions:

### *When PIA is Required*

A PIA will be conducted before implementing any project, system, or technology that involves:

- Collecting, using, disclosing, retaining, or destroying personal information.
- Acquiring, developing, or redesigning information systems or electronic service delivery systems that process personal information.
- Any activity that could have a high impact on the privacy or rights of individuals.

### *Objectives of the PIA*

The PIA aims to:

- Identify and assess potential privacy risks associated with the proposed project or initiative.
- Ensure that personal information is handled in a way that respects privacy rights and complies with Law 25.
- Recommend measures to eliminate or mitigate identified risks to an acceptable level.

### *Responsibilities*

- **Chief Privacy Officer (CPO):** Oversees the PIA process, ensuring it is conducted effectively and in accordance with legal requirements.
- **Project Leaders:** Collaborate with the CPO to provide necessary information and implement recommended measures.

- **Employees:** Participate in the PIA as required and adhere to the measures established to protect personal information.

## *PIA Process*

1. **Initiation:**
    - **Identification of the Project**: Any new initiative involving personal information must be reported to the CPO.
    - **Preliminary Analysis:** Determine if a PIA is necessary based on the scope and nature of the project.
2. **Assessment:**
    - **Description of the Initiative:** Detailed documentation of the project's objectives, processes, and technologies used.
    - **Analysis of Personal Information Involved:** Type, sensitivity, and volume of personal data collected or processed.
    - **Risk Identification**: Evaluate potential risks to privacy, including unauthorized access, loss, or misuse of data.
    - **Legal Compliance Check**: Ensure all activities comply with Law 25 and other applicable regulations.
3. **Risk Mitigation Measures:**
    - **Recommendations:** Develop strategies to mitigate identified risks, such as enhancing security measures or limiting data collection.
    - **Implementation Plan:** Outline steps to implement the recommended measures.
4. **Documentation:**
    - **PIA Report:** Compile all findings, analyses, and recommendations in a formal report.
    - **Approval**: Obtain sign-off from the CPO and relevant senior management before proceeding.
5. **Consultation with the CAI:**
    - If high residual risks remain after mitigation efforts, the Firm will consult the CAI for guidance before implementation.
6. **Monitoring and Review:**
    - **Ongoing Assessment:** Continuously monitor the project for new risks or changes in scope.
    - **Periodic Updates**: Review and update the PIA as necessary, especially if there are significant modifications to the project.

## *Record-Keeping and Retention*

- All PIA reports and related documents will be securely stored and retained in accordance with the Firm's data retention policies.
- Access to PIA documents is restricted to authorized personnel to maintain confidentiality.

### *Training and Awareness*

- **Employee Education:** Employees involved in projects requiring a PIA will receive training on the PIA process and their responsibilities.
- **Awareness Programs:** Regular updates and resources will be provided to ensure all staff understand the importance of privacy impact assessments.