MyLegacy
INSURANCE SERVICES

PROCEDURE IN CASE OF A VIOLATION OF PRIVACY

MyLegacy
INSURANCE SERVICES

PROCEDURE IN CASE OF A VIOLATION OF PRIVACY

TABLE OF CONTENTS

PROCEDURE IN CASE OF A VIOLATION OF PRIVACY

1. GENERAL PROVISIONS AND OBJECTIVES

MyLegacy Insurance Services is fully committed to protecting the personal information entrusted to us and ensuring compliance with applicable laws and regulations governing its management. As part of our commitment, we recognize the importance of implementing measures to address any potential breach or violation related to the protection of personal information.

While we have implemented robust protective measures, it is important to acknowledge that no system can guarantee absolute protection against breaches of personal information.

The objectives of this procedure are as follows:

- **Define Responsibilities:** Clearly outline the roles and responsibilities of individuals involved in managing and responding to breaches of personal information within MyLegacy Insurance Services. This includes designated personnel responsible for incident response, communication and compliance.
- **Establish Steps for Breach Response:** Provide a clear framework and guidelines for the actions to be taken in the event of a breach or violation of personal information. This includes prompt detection, containment, investigation, mitigation and recovery measures to minimize the impact on affected individuals and ensure appropriate handling of the incident.
- **Enhance Risk Management:** Foster a proactive approach to risk management by conducting risk assessments and implementing necessary controls and safeguards to prevent and mitigate breaches of personal information. This includes ongoing monitoring and periodic review of security measures to adapt to evolving threats and industry best practices.

- **Compliance with Regulatory Requirements:** Ensure strict adherence to legal and regulatory obligations pertaining to the protection of personal information. This includes timely reporting, documentation and cooperation with relevant authorities, as required by applicable laws and regulations.

By implementing this procedure, MyLegacy Insurance Services aims to uphold its commitment to the protection of personal information and to respond effectively in the event of a breach or violation. We continuously strive to enhance our security measures and maintain compliance with industry standards, demonstrating our dedication to safeguarding the privacy and confidentiality of personal information entrusted to us.

2. DEFINITIONS

A) Violation of Privacy (Breach of Personal Information):

A violation of privacy refers to any suspected or actual unauthorized access, consultation, collection, use or communication of personal information without proper authorization. It can also encompass incidents where personal information held by MyLegacy Insurance Services is stolen, lost or inadvertently disclosed due to procedural errors or operational failures. The severity of the breach is not a determining factor for applying this procedure.

B) Affected Person:

An affected person is an individual whose personal information is directly involved in the violation of privacy. They are the individuals to whom the personal information pertains.

C) Interested Person:

An interested person refers to any individual or entity indirectly affected by the privacy violation. This can include MyLegacy Insurance Services, its clients, suppliers, contractors, the general public or other organizations.

D) Personal Information:

Personal information refers to any information that relates to an individual and enables their identification.

E) Sensitive Personal Information:

Sensitive personal information includes data that requires a higher level of protection due to its nature, such as health status, government-issued identification documents, bank account details, credit card numbers or similar confidential information.

F) MyLegacy Insurance Services:

MyLegacy Insurance Services encompasses the organization itself, including its employees, management staff, contractors and representatives.

3. PROCEDURAL STEPS

In the event of a suspected or actual breach of data protection, MyLegacy Insurance Services follows a comprehensive set of procedural steps. These steps are designed to address breaches promptly and minimize potential harm.

Steps 3.1, 3.2 and 3.3 are to be carried out simultaneously or in quick succession, while step 3.4 focuses on long-term prevention and improvement strategies. Each breach should be treated seriously and an investigation should be initiated promptly.

3.1 Preliminary Assessment and Limiting the Breach

Upon learning of a breach or suspected breach, an employee, management staff member, contractor or representative of MyLegacy Insurance Services must take immediate action to limit the breach by:

a) Taking necessary measures to stop the unauthorized activity, including:

- Terminating the non-authorized practice.
- Retrieving the files.
- Shutting down the system responsible for the breach.
- Revoking or modifying access codes.
- Correcting deficiencies in material and computer security systems.

b) Informing the person responsible for the protection of personal information, who will:

- Assign a qualified individual to conduct an initial investigation.
- Investigate the breach and determine if a team comprising relevant stakeholders, senior management and the designated crisis coordinator is necessary.
- Determine, with or without the assistance of the team, which individuals need to be notified internally and potentially externally.
- Notify the Chief Compliance Officer.
- Notify the police if the breach involves theft or criminal activity.
- Thoroughly document the incident and preserve any evidence that could aid in identifying the cause or implementing corrective measures.

3.2 Assessment of Risk Associated with the Violation

To determine appropriate measures to implement, a risk assessment must be conducted considering the following factors:

3.2.1 Personal Information Involved

The nature and sensitivity of the personal information in question should be considered, as well as the foreseeable harm to affected and interested persons. Key considerations include:

- What specific elements of personal information were compromised?
- To what extent is the information sensitive?
- What is the context surrounding the personal information?
- Is the personal information adequately encrypted, de-identified or secured?
- How could the personal information be misused, particularly for fraudulent purposes?
- A thorough understanding of the type of personal information affected helps determine the necessary actions, parties to notify and the appropriate method of communication.

3.2.2 Cause and Extent of the Breach

Determining the cause and extent of the breach is crucial. The person responsible for the protection of personal information and/or the investigation team should verify:

- Is there a risk of ongoing unauthorized access or further compromise of the information?
- Was the information stolen or lost and if stolen, was it the primary target?
- Has the personal information been recovered?
- What measures were taken to mitigate harm or damages?
- Is the breach an isolated incident or indicative of a systemic problem?

3.2.3 Affected Persons

Identifying the individuals affected by the breach is essential. This step involves determining:

- Who is directly impacted by the breach (e.g., employees, clients, suppliers)?
- The extent of personal information affected by the breach.
- Potential recipients of the compromised personal information.

3.2.4 Foreseeable Harm Resulting from the Breach:

The person responsible for the protection of personal information and/or the investigation team must assess the foreseeable harm to affected and interested persons. Key considerations include:

- Is there a link between the unauthorized recipients and the affected individuals?
- What potential harm could be inflicted on the affected and interested persons (e.g., physical safety risk, identity theft, financial loss, reputation damage)?
- What potential harm could the breach cause for MyLegacy Insurance Services (e.g., loss of trust, financial risks, legal actions)?

3.3 Notification of the Breach

Determining when and how to notify affected individuals and interested parties can be challenging, as each situation requires a case-by-case analysis. The following factors should be considered:

3.3.1 Notice to Affected and Interested Persons

To decide whether affected and interested persons should be notified, the following factors should be considered:

- Legal and contractual obligations.
- Risks of harm to affected and interested persons.
- Suspected identity theft, misappropriation of identity or fraud.
- Risk of personal injury or reputation damage.
- Possibility of avoiding or mitigating potential harm.

3.3.2 How and When to Notify Affected and Interested Persons?

Affected and interested persons should be notified as quickly as possible, unless advised otherwise by law enforcement officials to avoid compromising an investigation. Direct

notification through telephone, mail, email or in-person communication is preferred, while indirect notification methods (e.g., website or public notice) are not recommended.

The notice should contain relevant information, which may include:

- Brief description and timing of the breach.
- Description of the compromised personal information.
- Steps taken to control or reduce harm.
- Assistance provided by MyLegacy Insurance Services and recommendations for individuals to protect themselves (e.g., credit monitoring, updating identification documents).
- Sources of information for individuals to protect themselves against identity theft and misappropriation of identity.
- Contact information for a MyLegacy Insurance Services representative who can answer questions and provide further assistance.
- Reporting of the breach to the privacy commissioner.
- Instructions on how affected individuals can provide feedback or share their concerns.
- Contact information for the privacy commissioner's office.

3.3.3 Notification of Other Parties

The person responsible for the protection of personal information and/or the investigation team should also consider notifying other relevant parties, including:

- Law enforcement authorities in cases involving theft or criminal activity.
- Insurance companies or other contractual obligations.
- Professional organizations or regulatory agencies as required by applicable standards.
- Financial institutions, including insurance companies, if their cooperation is necessary for communicating with affected individuals.

- Any other relevant stakeholders.

3.4 Future Prevention

Once immediate measures have been taken to mitigate the breach's risk, the person responsible for the protection of personal information and/or the investigation team must investigate the root causes of the incident and develop a prevention plan, if necessary. This step involves:

- Verifying physical and technical security measures.
- Reviewing and updating policies and procedures.
- Assessing training practices for employees.
- Evaluating provider practices.

Please note that this breach procedure is subject to regular review and may be updated based on changes in regulations, industry best practices or internal policy changes or enhancements.

4. RESPONSIBILITIES

We assign different responsibilities to individuals or groups for implementation of the breach procedures. Here's a breakdown of how we operate on our responsibilities for you to better understand the flow and structure with which we work and that the information you provide is secure and safe with MyLegacy Insurance Services.

4.1 Management

Members of our executive committee adopt the present procedure and name the person responsible for the protection of personal information as responsible for the application and implementation of the procedure.

4.2 Person responsible for the protection of personal information

Whoever is responsible in our team would coordinate all investigations regarding a breach and sets up an investigative team. He/She would also keep the management aware of activities on a regular basis and seeks their approval when necessary. They also ensure that the present procedure is delivered and communicated to all employees and produces an annual report of his activities and presents it to the executive committee.

4.3 Management staff members

Management staff members respect the present procedure and ensure it is communicated to their employees. They take all necessary means to limit, without delay, any violation they are made aware of and immediately report it to the person responsible for the protection of personal information. At his/her request, the management staff is part of the team in charge of the investigation.

4.4 Employees

Employees respect and comply with the present procedure. They advise their superior immediately or, if they cannot, the person responsible for the protection of personal information, of any breach. They take necessary measures to limit it immediately. At the request of the person responsible for the protection of personal information, they are part of the team in charge of the investigation.

4.5 Team in charge of the investigation

The persons appointed by the person responsible for the protection of personal information to be part of the investigation team must participate in each of the steps described in detail in the present policy.

4.6 Communication Plan

In the event of a breach, effective communication is crucial to minimize the impact and maintain transparency. MyLegacy Insurance Services has established a comprehensive

communication plan to ensure that the right stakeholders are informed in a timely manner. The plan includes:

- **Internal Communication:** Key members of the organization, including management staff, the person responsible for the protection of personal information and the investigation team, will be notified promptly about the breach. Clear communication channels and protocols will be followed to share relevant information and updates internally.
- **External Communication:** Depending on the nature and severity of the breach, MyLegacy Insurance Services will communicate with external parties, including affected individuals, regulatory authorities, legal counsel and any other relevant stakeholders. The communication will be conducted in accordance with legal requirements and best practices, ensuring that accurate and consistent information is provided.
- **Key Messages:** The communication plan includes predefined key messages to address the breach incident. These messages focus on providing clear and concise information about the breach, the potential impact on affected individuals, the steps taken to mitigate the breach and any recommended actions for individuals to protect themselves.
- **Timelines:** The communication plan establishes specific timelines for notifying relevant parties. It ensures that notifications are provided within the required timeframes mandated by applicable laws and regulations. The plan also includes provisions for ongoing communication and updates as the investigation progresses and further information becomes available.

4.7 Documentation and Record-Keeping

Accurate and comprehensive documentation is essential for managing and responding to a breach effectively. MyLegacy Insurance Services maintains a robust documentation

and record-keeping process to ensure the proper handling and retention of breach-related information. The process includes:

- **Incident Documentation:** A dedicated incident response team, led by the person responsible for the protection of personal information, will document all relevant details of the breach incident. This includes a description of the breach, the date and time of occurrence, the affected systems or data and any initial actions taken to mitigate the breach.
- **Evidence Preservation:** The documentation process emphasizes the preservation of evidence related to the breach. This includes capturing screenshots, logs and any other relevant information that may assist in determining the cause of the breach and identifying potential vulnerabilities.
- **Record Retention:** All documentation and records related to the breach will be securely retained for the required period as stipulated by applicable laws and regulations. This ensures that the information is available for future reference, compliance audits and potential investigations.

4.8 Remediation and Follow-Up

Following a breach, MyLegacy Insurance Services is committed to taking prompt and effective measures to remediate the breach and prevent similar incidents from occurring in the future. The organization follows a systematic approach that includes:

- **Root Cause Analysis:** The investigation team, in collaboration with relevant stakeholders, conducts a thorough analysis to identify the root causes and contributing factors of the breach. This analysis helps to determine any weaknesses or gaps in existing security measures and processes.
- **Corrective Actions:** Based on the findings of the root cause analysis, MyLegacy Insurance Services implements appropriate corrective actions to address the identified vulnerabilities. This may involve enhancing security controls, updating

policies and procedures, providing additional training and awareness programs or making necessary changes to systems and infrastructure.

- **Ongoing Monitoring and Assessment:** To ensure the effectiveness of the implemented remediation measures, MyLegacy Insurance Services establishes an ongoing monitoring and assessment process. This includes regular reviews and audits of security controls, periodic risk assessments and vulnerability scanning. The organization remains vigilant in identifying and addressing any emerging threats or potential areas of improvement.

4.9 Training and Awareness

MyLegacy Insurance Services recognizes the importance of continuous training and raising awareness among employees to prevent, detect and respond to breaches effectively. The organization maintains a comprehensive training and awareness program that includes:

- **Employee Training:** All employees undergo regular training sessions to enhance their understanding of data protection principles, privacy laws and best practices for safeguarding personal information. The training covers topics such as identifying potential security risks, handling sensitive data, incident reporting procedures and the importance of maintaining a culture of privacy and data protection.
- **Awareness Campaigns:** MyLegacy Insurance Services conducts periodic awareness campaigns to reinforce privacy and security practices. These campaigns may include internal communications, newsletters, posters and other resources that promote a heightened sense of responsibility and vigilance regarding personal information.
- **Incident Response Training:** Key personnel, including the investigation team and relevant management staff, receive specialized training on incident response protocols. This training ensures they are equipped to respond promptly and

effectively in the event of a breach, following established procedures and minimizing the potential impact.

4.10 Compliance Monitoring and Review

To maintain compliance with privacy laws, regulations and industry standards, MyLegacy Insurance Services maintains a robust compliance monitoring and review process. This involves:

- **Regular Audits:** Internal audits are conducted periodically to assess compliance with breach procedures and related policies. These audits evaluate the effectiveness of security controls, incident response processes, training programs and documentation practices. Any identified non-compliance or areas for improvement are addressed promptly.
- **External Assessments:** MyLegacy Insurance Services may engage third-party experts to conduct external assessments of its breach procedures and data protection practices. These assessments provide an independent evaluation of compliance and help identify potential areas for enhancement.
- **Regulatory Compliance:** The organization stays updated on relevant privacy laws and regulations, ensuring ongoing compliance with applicable requirements. This includes monitoring changes to legislation, staying informed about evolving best practices and promptly implementing any necessary updates to policies and procedures.

By incorporating these components into the breach procedures, MyLegacy Insurance Services demonstrates its commitment to effectively managing and responding to breaches of personal information while ensuring compliance with legal and regulatory obligations.