Data Protection

guard.me International Insurance

January 10, 2024

Table of Contents

Data Protection

This policy is about the organization's approach for secure data collection, storage, and processing.

Information Classification: Public

1.0 Purpose

This purpose of this policy is to identify how guard.me International Insurance protects the data it collects, stores, or processes.

2.0 Scope

This policy applies to all employees and contractors of guard.me International Insurance who have duties and responsibilities that involve the collection, storage, use, disclosure, retention, or disposal of the data of guard.me International Insurance’s employees, customers, and other third parties. This policy also applies to all data assets of guard.me International Insurance, whether owned or provided by a third party.

These data assets include, without limitation, intellectual property (IP), personally identifiable information (PII) and personal health information (PHI) for employees, insureds and other third parties (collectively personal information (PI)), as well as any information labelled Confidential or Restricted, together with other non-public data or information assets deemed the property of guard.me International Insurance.

3.0 Roles and Responsibilities

3.1 Data Owners

A data owner is a person who is ultimately responsible for the data and information being collected and maintained by their department or division. All data within guard.me International Insurance must be assigned a data owner, either directly or indirectly, through their roles and responsibilities in the organization. The responsibilities of the data owners include defining data retention and destruction requirements and making sure they are enforced.

3.2 Data User

A data user is a person or an entity that interacts with, accesses, uses or updates data to perform a task authorized by the data owner. Data users must use data in a manner consistent with the purpose intended and comply with this policy and all policies applicable to such data use.

3.3 Data Subject

A data subject is a natural person about whom guard.me International Insurance holds PI and who can be identified, directly or indirectly, by reference to that PI.

4.0 Policy

4.1 Privacy and Security Compliance

- With respect to data privacy compliance, guard.me International Insurance adheres to all regulatory, legal, and contractual requirements that apply to the information of data subjects (employees, customers, and other third parties) that guard.me International Insurance collects, stores, processes, or deletes
- guard.me International Insurance has a program in place to identify legislated and other updates to these requirements and implement changes as necessary

4.2 Data Collection

- guard.me International Insurance only collects or creates personal information that is necessary for the performance of guard.me International Insurance's obligations, or the exercise of guard.me International Insurance's rights
- guard.me International Insurance must tell an individual from whom guard.me International Insurance is collecting PI:
  - The purpose for collecting it
  - The legal authority for collecting it
  - The title and contact details of the individual designated to answer questions about guard.me International Insurance's collection of PI

4.3 Data Accuracy

- guard.me International Insurance makes every reasonable effort to ensure the accuracy and completeness of any PI collected, stored or processed

4.4 Data Correction

- guard.me International Insurance aids data subjects and others in accessing or correcting personal information as well as deleting specific data elements (i.e., secondary email address, etc.)
- If guard.me International Insurance receives written notification to correct or annotate any personal information, guard.me International Insurance will update the information within three business days of the date of receipt, unless a specific contractual clause requires guard.me International Insurance to escalate the request to the designated privacy contact at the client's educational institution
- Within five business days of correcting or annotating any personal information, guard.me International Insurance provides the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made, guard.me International Insurance disclosed the information being corrected or annotated, unless a specific contractual clause requires guard.me International Insurance to escalate the request to the designated privacy contact at the client's educational institution

4.5 Data Storage

- All data is to be kept confidential and secure
- Data at rest should be kept in an encrypted state
- Any data at rest maintained on behalf of guard.me International Insurance by a third party must be geographically located in Canada

4.6 Data Use

- guard.me International Insurance does not use, sell or commoditize any customer data stored in its tenant or customer profile metadata
- guard.me International Insurance does not merge, match or aggregate any data asset with that of any other client or user

4.7 Data Access / Disclosure

- Access to stored data is limited to those individuals with a need to know for the purpose of providing guard.me International Insurance services
- Any data disclosure to authorized third parties is logged for audit purposes
- Data should only be transmitted in an encrypted state
- System identifiers that allow access to the data in an unencrypted state are reviewed on an annual basis
- Personal social media and email accounts are not to be used for communication of any guard.me International Insurance business
- PII / PHI must not be disclosed to any third party without written authorization from the insured or their authorized agent
- If an insured provides guard.me International Insurance with a signed authorization to release any PII / PHI, guard.me International Insurance will log the request, including the expiry date of the authorization
- Before releasing any information or records, guard.me International Insurance personnel must validate the details of each release against the Release of Information form signed by the insured
- Each release of information is logged in GMIS as a Note

- Outside of the administration of services provided by the policy, and the adjudication of claims, the use of email for sending PII or PHI to external third parties is not allowed

4.8 Data Retention

4.8.1 Retention of Business-Sensitive and Financial Information

- guard.me International Insurance's business-sensitive and financial information should be retained per the schedule below.

Data/Record Types	Retention Period
Accounts Payable Ledgers and Schedules	Ten years
Accounts Receivable Ledgers and Schedules	Ten years
General Ledgers	Permanent
Annual Audit Reports and Financial Statements	Permanent
Bank Statements	Seven years
Chart of Accounts	Permanent
Stock and Bond Records	Permanent
Contracts and Leases	Seven years after expiration
Correspondence (legal)	Permanent
Employee Payroll Records	Permanent
Contractor Payment Records	Seven years
Insurance Records	Permanent
Invoices to Customers	Seven years
Invoices from Vendors	Seven years
Employee Expense Reports	Seven years
Board Meeting Minutes	Permanent
Emails – Internal and External	Ten years
Electronic Documents	Depends on the subject matter
Legal Files and Papers	Seven years after the closing of the matter

Risk Assessment Reports	Seven years
Internal Audit Reports	Ten years

4.8.2 Retention of PII) and Personal Health Information (PHI)

- All PII and PHI data should be retained for as long as there is a business purpose or a legal requirement to do so.

4.8.3 Retention of Customer Data

- All active customer data should be retained for the following periods, according to CLHIA guidelines:
    - If no claim was made, the data (electronic and paper) is retained until the end of the last insurance interaction plus seven years.
    - If a claim was made, the data (electronic and paper) is retained until the end of the last insurance interaction plus 15 years.
- Customer data retention policies may be implemented against customer data on an ad-hoc basis as may be agreed between guard.me International Insurance and the customer.

4.9 Data Disposal

4.9.1 Customer Data Disposal

- Disposal of customer data should be carried out in accordance with the contractual agreement between guard.me International Insurance and the customer. In the absence of any contractual agreement, an automatic script or manual script (for ad-hoc requests) should be initiated on any guard.me International Insurance platform containing customer data. This activates secure deletion of customer data on the platform.

4.9.2 PII / PHI Disposal

- All electronic documents containing PII or PHI must be purged upon reaching its retention life span. This includes all temporary files created through processing PII or PHI.
- All printed material must be shredded prior to disposal.
- As identified in Section 6.7 of the Removable Media Policy, when removable media is repurposed for use, any PII / PHI that it contains will be securely overwritten by industry standard tools and technology.

4.9.3 Other Data Disposal, Including guard.me International Insurance’s Business-Sensitive Information (BSI)

- All electronic documents containing guard.me International Insurance’s BSI should be purged upon reaching its retention life span. This includes all marketing materials.
- All printed material must be shredded prior to disposal.

4.9.4 Data De-Identification

- All data, once processing in the production environment is completed, is fully anonymized before being used outside of the production environment, including for development, testing or QA purposes.

4.9.5 Logging of Data Disposal

- When electronic data is disposed of, guard.me International Insurance keeps a log of the data disposed, date, affected media, etc.
- When printed material is disposed of, it is placed in a secure cabinet for pick up by guard.me International Insurance's third party vendor. When the materials are picked up and shredded, the vendor provides a

Certificate of Destruction to guard.me International Insurance identifying the date and other details of the disposal.

4.9.6 Log Files

Our organization recognizes the importance of protecting sensitive data within log files and should follow the guidelines set forth in ISO 27701 6.9.4.2 - Protection of Log Information. In order to ensure the protection of sensitive data within log files, the following is our de-identification policy:

- De-Identification Process: Our de-identification process should follow the best practices of ISO 27701, and involve the removal or masking of any sensitive information that could be used to identify an individual or entity. This should include, but is not limited to, names, addresses, social insurance numbers, phone numbers, email addresses, and financial information.
- All tools and technologies should be configured such that personal information is not captured in any log file.
- Manual De-Identification: In some cases, our trained staff should manually review the log files and remove or mask any sensitive information.
- Retention Policy: Our organization should retain log files only for as long as required for business purposes or as required by law. After the retention period, the log files should be securely deleted.
- Data Access: Access to log files should be restricted to authorized personnel who have a legitimate business need to access the information. guard.me International Insurance should monitor access to log files and keep a record of who has accessed them.

By following this de-identification policy, guard.me International Insurance will be able to protect sensitive data within log files and ensure that it is not used inappropriately. guard.me International Insurance remains committed to continually reviewing and updating our policies and procedures to align with the latest best practices and standards, including ISO 27701.

4.10 Suspension of Disposal in the Event of Litigation or Claims

- In the event guard.me International Insurance is served with any subpoena or request for documents or any employee becomes aware of a governmental investigation or audit concerning guard.me International Insurance or the commencement of any litigation against or concerning guard.me International Insurance, such employee should inform Management. Any further disposal of documents should be suspended until Management with the advice of counsel determines otherwise. Management should take such steps as are necessary to promptly inform all staff of any suspension in further data disposal.

4.11 Data Subject Access Rights

guard.me International Insurance complies with all data subject access rights, including:

- Right of Access by the Data Subject: GDPR; ISO 27701
- Right to Rectification: GDPR; ISO 27701
- Right to Erasure: GDPR; ISO 27701
- Right to Restriction of Processing: GDPR
- Right to Data Portability: GDPR; ISO 27701
- Right to Object: GDPR
- Responding to Requests Not to be Subject to Automated Decision Making: GDPR; ISO 27701

We accept all data subject access rights and respond in accordance with our Data Subject Rights Policy.

5.0 Policies & Procedures

For more information on implementing this policy, see the following:

- Data Accuracy and Completeness Policy
- Data Consent and Disclosure Policy
- Data Protection Impact Assessment (DPIA) Procedure
- Data Relocation Scenarios
- Data Subject Rights Policy
- International Transfers of Personal Data Procedure

6.0 Enforcement

Any employee found to be in violation of, or to have violated, this policy may be subject to disciplinary action in line with the Disciplinary Policy.