Data Protection Policy

1 BACKGROUND AND OBJECTIVES

This policy applies to all employees at RiskPoint Group (the "Company") on a global basis. The Company gather and use certain information about various parties. These can include customers, suppliers, brokers, carriers, business contacts, employees and other people the Company has a relationship with or may need to contact.

This policy describes how Personal Data must be collected, handled and stored to meet the Company's data protection standards, and comply with applicable law.

This policy is designed to ensure that the Company:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

It applies to the processing of all data the Company holds, including data relating to Data Subjects, such as:

- Names of individuals
- Social security numbers
- Postal addresses
- Email addresses
- Telephone numbers
- Medical records
- Date of birth
- Gender

This policy helps to protect the Company from data security risks, including breaches of confidentiality and reputational damage. The former is when information is transferred inappropriately whereas the latter reflects what could happen is unauthorized third parties gained access to sensitive data.

2 DATA

Data comes in various forms, and with different levels of legal protection. Personal Data is subject to a high level of legal protection. Special Categories of Personal Data is prohibited to process by default (as detailed in European regulation).

'Personal Data' means any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

'Special Categories of Personal Data' means any information regarding the private information of an identified or identifiable natural person. This relates to a person's ethnical origin, political opinion, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data or data concerning sex life or sexual orientation.

3 DATA PROTECTION LAW AND RIGHTS OF THE DATA SUBJECT

This policy will address the requirements and principles detailed in European regulation being the General Data Protection Regulation (EU/2016/679), applicable for organizations domiciled and operating within the EU, as well as organizations in other countries who processes personal data of EU Data Subjects. These requirements and principles describes how organizations – including the Company – must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other media. As the Company has operations in other territories outside the European Economic Area, local regulation must be adhered to for these operations as well as following the principles of this policy.

The Data Protection Regulation is underpinned by eight principles for the handling of Personal Data, of which the Company strive to follow. Personal Data must;

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant, and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Be processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

The Data Protection Regulation outlines eight distinct rights that all Data Subjects are entitled to and which the Company must uphold through our data practices. The eight rights are:

- The right to information
- The right of access
- The right to rectification
- The right to erasure
- The right to restriction of processing
- The right to data portability
- The right to object
- The right to avoid automated decision-making

4 RESPONSIBILITIES

Company employees have a responsibility to ensure that data is collected, stored, handled and deleted appropriately.

As the Company's IT-platform is hosted and maintained by a third party vendor (the Processor); a data processing agreement has been agreed, to secure the lawfulness and security of the data processing conducted by the Processor, of which the Company holds control. This agreement addresses data storage, back-up procedures, erasure and destruction of data, as well as confidentiality.

Each team within the Company who handles Personal Data must ensure that it is handled and processed in line with this policy and data protection principles. However, the following people have key areas of responsibility:

- The managing directors are ultimately responsible for ensuring that the Company meets its legal obligations
- The CTO is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the company is considered using to store or process data.

5 RETRIEVING DATA

Prior to any processing of Personal Data, the correct legal basis must be held to retrieve such data. This can be completed by obtaining the consent of the Data Subject, for the handling of one or more specific purposes, or, if the processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.

For the processing of Special Categories of Personal Data, such as medical information, which is needed in order to process certain types of claims; a declaration of consent form must be sent to the relevant party, for signature, and returned before this type of data can be collected and processed.

The Personal Data shall only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The Personal Data shall

be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

The key principle before retrieving and processing Personal Data, is to make sure that the Data Subject fully understands how and to what purpose their Personal Data is being processed.

6 PROCESSING

When the correct legal basis is obtained, procedures must be followed in order to secure a lawful, fair and transparent processing:

- The only people accessing the data covered by this policy should be those who specifically need it for their work
- Personal Data obtained within the European Economic Area should never be transferred outside the European Economic Area or the UK, unless cleared by the CTO and the Operations Manager
- Employees must keep all data secure, by taking sensible precautions and following the guidelines below;
    - Strong passwords must be used and should never be shared.
    - Personal Data must not be disclosed to unauthorized people, neither internally or externally.
    - Employees must ensure the screens of their computers are always locked when left unattended.
    - Employees must not save copies of Personal Data to their own computers or mobile devices.
    - Data must be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
    - Employees must request help from their manager if they are unsure about any aspects of data protection.

A key part of making sure processing is secure is to specifically secure emails. As such, all emails are encrypted according to industry standards. For sensitive data, there is an option of adding another layer of encryption. Employees are required to use this encryption when handling personal or sensitive data.

7 DATA STORAGE

This section describes how and where data must be stored. Questions about storing data safely can be directed to the CTO or the Director of Finance & Operations.

When data is stored on paper, it should be kept in a secure place where unauthorized people cannot gain access to it.

The guidelines also apply to data that is usually stored electronically but has been printed:

- Employees should make sure paper and printouts are not left unattended
- Data printouts should be disposed of securely when no longer required

When data is stored electronically, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:

- Data must be protected by strong passwords that are changed regularly (system access prompts this to occur every three months) and never shared between employees.
- If data is stored on physical media (like usb-drives) these must be stored securely when not in use.
- Data should only be stored on designated drivers and servers, and not be stored locally on any terminal, personal computer or other mobile device (tablets, smart phones).
- Servers are to be located in a secure location, away from general office space.
- Data is backed up frequently. Those backups are tested regularly, in line with the company's standard backup procedures.
- All servers and computers containing data should be protected by approved security software and firewall.

8 DATA ACCURACY

It is the responsibility of all employees who work with Personal Data to take reasonable steps to ensure it is kept accurate and up to date.

- Data is held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should strive to ensure data is updated. For instance, by confirming a customer's details when in contact.
- The Company will make it easy for Data Subjects to update information held about them.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored phone number, it should be removed.

9 SUBJECT ACCESS REQUESTS

All individuals who are the subject of Personal Data held by the Company are entitled to:

- Ask what information the Company holds about them and why.
- Be informed of how to keep it up to date.
- Be informed of how the Company is meeting its data protection obligations.

If an individual contacts the Company requesting this information, this is called a subject access request. Any employee who receives a subject access request must promptly forward that request to the CTO, who will then be responsible for the request.

The information requested, must be provided to the Data Subject within one month of receiving the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Company shall inform the Data Subject of any such extension within one month of receiving the request, together with the reasons for the delay.

10 DATA RETENTION

Personal Data must only be stored and processed for as long as it is necessary for the purpose of which it was collected. When no longer needed, the data must be deleted or anonymized to such a degree that it no longer qualifies as Personal Data. Some jurisdictions have minimum data retention periods for specific types of Personal Data, such as employee files, which must be adhered to. After the minimum retention period, the data must be deleted.

11 PERSONAL DATA BREACH

'Personal Data Breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. In the event of a Personal Data Breach, the Company must without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the relevant national supervisory authority (See Appendix 1), unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

A Personal Data Breach can happen at any level within the Company. Any Company employee who suspects a Personal Data Breach has occurred must notify the Director of Finance and Operations immediately after becoming aware of the breach or potential breach. The notification must be sent via email and should contain (as a minimum):

- a description of the Personal Data breach (why is it a breach?)
- information about when the breach was detected
- information about when the breach happened

It is responsibility of the Director of Finance & Operations to conduct the reporting to the respective authorities and involved parties. Employees should not be contacting the Data Subjects without the Director of Finance & Operations involvement.

12 DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, Data Protection Regulation allows Personal Data to be disclosed to law enforcement agencies without the consent of the Data Subject. Under these circumstances, the

Company will disclose requested data. However, the Company will assess (with appropriate advice) and seek to verify that the request is legitimate.

13 DATA ETHICS

Data ethics principles are key part of this Data Protection Policy to ensure that we comply with applicable Data Protection Regulation when Personal Data is processed and stored, but more importantly, that the processing of any type of data are in alignment with our core values of trust, openness and honesty, alongside respect and tolerance.

Data is and will remain the foundation of the insurance industry and ethical considerations of collection, storage, usage and sharing data is a key element of acting as a responsible insurance business. By respecting the privacy and confidentiality of our customers, business partners, and stakeholders the Company aspire to build long-term relationships, offer bespoke insurance products by processing only the data necessary for the purpose of which they are collected. This includes:

- Personal Data about policyholders, claimants, business relations, job applicants and employees
- Non-Personal Data about our operating assets and other business-related information

The Company collects data directly from various sources:

- Customers being the insured and/or policyholder
- Employees
- Beneficiary
- Insurance brokers and agents
- Public and private registers

The Company does not sell or buy Personal or non-Personal Data.

Version: 6
Dated: February 5, 2025

Appendix 1 – National Data Protection Authorities

Australia - The Information Commissioner, under the Office of the Australian Information Commissioner (OAIC)

Belgium - Autorité de protection des données / Gegevensbeschermingsautoriteit

Canada – The Office of the Privacy Commissioner of Canada

Denmark - Datatilsynet

Finland - Office of the Data Protection Ombudsman**Germany -** Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Italy - Garante per la protezione die dati personali (GPDP)

Netherlands - Autoriteit Persoonsgegevens

Norway - Datatilsynet

Singapore – The Personal Data Protection Commission (PDPC)

Spain - Agencia Española de Protección de Datos (AEPD)

Sweden - Datainspektionen

Switzerland - Federal Data Protection and Information Commissioner (FDPIC)

United Kingdom - Information Commissioner's Office (ICO)

United States – The US Federal Trade Commission (FTC)