Fusion Specialty Insurance Group
www.fusion.insure.com
Suite 25.02, 259 George St
Sydney NSW 2000, Australia

Data Protection and Privacy Policy

Introduction

Data protection and data privacy is a growing issue that concerns companies who must take more measures to mitigate the risks of breaches of the law. Therefore, it is essential that Fusion (hereinafter: "Company") acts in compliance with the applicable legal provisions as well as in accordance with its ethical values. This data protection and privacy policy (hereinafter: "Policy") sets out how the Company seeks to protect personal data and ensure that its staff understand the rules governing the use of the personal data to which they have access in the course of their work.

The persons involved are clients, employees, staff members and other third parties.

The General Data Protection Regulation (GDPR), as supplemented by the data protection act 2018 (DPA), is the main piece of legislation that governs how the Company collects and processes personal data. Failure to comply with this may involve a severe economic and/or reputational impact.

Purpose

This Policy sets the general framework for the compliance of the Company regarding the obligations related to the data protection.

Scope

This Policy is applicable to all entities of the Company.

This Policy applies to all employees and any person directly or indirectly linked to the Company by control.

Supporting Policies and Procedures

This Policy is part of a wider internal framework of the Company. The following documents are linked to the data protection:

- Privacy notices;
- Information/Cyber Security Policy
- Data Retention Policy
- Cookies Policy

Policy Statement

Definitions

- 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, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- Processing: Means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- Controller: Means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

- Processor: Means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

- Recipient: Means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

- 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.

- Consent of the data subject: Means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Responsibilities

Data Protection Officer

The Company has decided to appoint a Data Protection Officer (hereinafter: “DPO”) in order to ensure the compliance with the legal requirements applicable to the Company.

The DPO is responsible of the good conduct of the data protection as defined in this Policy.

In case of delegation, the DPO remains the responsible person in charge of the good execution of the tasks related to the data protection framework.

The contact details of the DPO are the following: Gayle Robertson (gayle@fusion.insure)

The DPO in responsible to:

- Inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the applicable legal framework;
- Monitor compliance with the applicable legal framework and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- Provide advice where requested as regards the data protection impact assessment and monitor its performance;
- Cooperate with the supervisory authority; and
- Act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation, and to consult, where appropriate, with regard to any other matter.

In its performance, the DPO will have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Compliance

The compliance department acts as a point of contact for all the data protection matters in case the DPO is no longer available.

If the DPO is not part of compliance department, he will ensure the good and coherent collaboration with the compliance department of the execution and implementation of the data protection measures.

Principles

The Regulation sets out the following principles with which any party handling personal data must comply. Article 5 in the GDPR states that all personal data the Company respect when processing data.

Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly, and in a transparent manner.

Processing personal data will only be lawful where at least one of the following lawful bases applies:

- The data subject has given their consent for one or more specific purposes;
- The processing is necessary for the performance of a contract to which the data subject is a party;
- To comply with the Company's legal obligations;
- To protect the vital interests of the data subject or another person;
- To perform tasks carried out in the public interest or the exercise of official authority; and/or

- To pursue the Company's legitimate interests where those interests are not outweighed by the interests and rights of data subjects.

The Company must always be able to justify the processing based on the above basis.

Purpose limitation

The Company must only collect and process personal data for specified, explicit and legitimate purposes that have been communicated to data subjects before the personal data have been collected. The Company must ensure that it does not process any personal data obtained for one or more specific purposes for a new purpose that is not compatible with the original purpose. Where the Company intends to do so, it must inform the data subjects before using their personal data for the new purpose and, where the lawful basis relied upon for the original purpose was consent, obtain such consent again.

Data minimization

Any processing of personal data must be limited, both quantitatively and qualitatively, to what is necessary for the achievement of the purposes for which the data is lawfully processed. This must be taken into account during the initial data collection. If the purpose permits, and the effort is in proportion to the objective pursued, anonymized or statistical data must be used.

Accuracy

The personal data stored must be objectively correct and, if necessary, up to date. Appropriate measures must be adopted to ensure that incorrect or incomplete data is deleted, corrected, supplemented or updated.

Storage limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

The Company must not keep personal data in a form which permits the identification of the data subject for longer than needed for the legitimate business purpose or purposes for which it is originally collected including for the purpose of satisfying any legal, accounting or reporting requirements.

The Company will maintain retention policies and procedures to ensure personal data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

The Company will take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

The Company will ensure data subjects are informed of the period for which data is stored and how that period is determined.

Integrity and confidentiality

The personal data that the Company collects and processes must be secured by appropriate technical and organizational measures against accidental loss, destruction or damage, and against unauthorized or unlawful processing.

Accountability

In its qualification as a controller, the Company is ultimately responsible and is able to demonstrate compliance with all applicable data protection laws and regulations.

Data subject rights

The GDPR provides the following rights to the data subjects. Those are the following:

- Access of personal data – right of the data subject to ask what personal data the Company processes and request copies of such personal data;
- Rectification of personal data – right of the data subject to ask to rectify or update personal data that is inaccurate or incomplete;
- Erasure of personal data – right of the data subject to ask to delete his/her/their personal data in certain instances;
- Restriction of processing – Under certain circumstance (such as when the data subject questions the accuracy of the personal data the Company holds on him/her/them or the lawfulness of its processing) right of the data subject to ask to stop processing such data until his/her/their request is resolved;
- Data portability – in certain cases, right of the data subject to send an electronic copy of his/her/their personal data directly to he/she/them or to another organization;
- Object – right of the data subject to object to any processing of his/her/their personal data, including profiling, based on the ground of legitimate interest; and
- Withdraw – where processing of personal data is based on the data subject's consent – he/she/they may at any time withdraw his/her/their consent (without affect however any processing the Company did before withdrawal).

Privacy notice

The Company takes all appropriate measures to ensure providing data subjects with a data protection notice before processing their personal data. It is as well ensure this is done in a clear manner and including the following minimum information:

- The identity and contact details of the controller (i.e. the person who determines the purposes

and manner in which personal data are processed) and where applicable, the DPO;

- The purposes and legal basis for the processing, including the legitimate interest(s) pursued by the data controller if this is the legal basis for processing;
- The recipients or categories of recipients of the personal data;
- The details of any international transfers around thew globe and how to obtain a copy of the relevant safeguards;
- The retention period for personal data, or where this is not possible, the criteria used to determine this period;
- The existence of the data subject's rights and the right to withdraw consent;
- The right to lodge a complaint with the competent data protection authority;
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide such information; and
- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing.

Processing of personal data by third party (sub)processors

The Company ensures implementing all contractual and regulatory obligations foreseen under Article 28 of GDPR when entering into business relationships with third-party (sub)processors, including a written data processing agreement to be entered into and setting out the following specific data processing provisions:

- The subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller;
- The obligation upon the processor to only process personal data on documented instructions from the controller (unless required to do so by Union or Member State law to which the processor is subject in which case the processor must inform the controller of that legal requirement before processing);
- The obligation upon the processor to ensure that staff authorized to process the personal data has committed to (or is under an appropriate statutory obligation of) confidentiality;
- The obligation upon the processor to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk;
- The prohibition of the processor to engage another (sub)processor without prior specific or general written authorization of the controller;
- In case of engaging with another (sub)processor, the obligation upon the processor to set out in a written agreement with such (sub)processor the same data protection obligations than those set out between the controller and the processor;
- The obligation upon the processor to assists the controller in implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's

obligation to respond to requests for exercising the data subject's rights as well as in ensuring compliance with the controller's data protection obligations;

- The obligation upon the processor to delete or return all the personal data to the controller after the end of the provision of services, and deletes existing copies (unless Union or Member State law requires storage of the personal data upon the processor); and
- Obligation upon the processor to make available to the controller all necessary information to evidence compliance with the above listed requirements and allow and contribute to audits, including inspections conducted by the controller or another mandated auditor.

Record of processing activities

The Company ensures maintaining a record of processing activities containing the following information:

- The name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the DPO;
- The purposes of the processing;
- A description of the categories of data subjects and of the categories of personal data;
- The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations;
- Where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, as the case may be, the documentation of suitable safeguards implemented;
- Where possible, the time limits for erasure of the different categories of data; and
- Where possible, a general description of the technical and organizational security measures implemented.

Data protection impact assessments

The Company must ensure its having appropriate procedures in place to carry out an impact assessment when a type of processing (in particular using new technologies) may present a high risk to the rights and freedoms of natural persons.

Security of processing

The Company ensures implementing appropriate technical and organizational measures to ensure the level of security that is appropriate to the Company's data breach exposure (including among others, pseudonymization and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner, a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing, etc.).

International transfers

The Company ensures that any transfer of personal data to third-countries is undertaken in line with the conditions laid down under the applicable data protection laws and regulations. Where personal data is transferred outside the EEA/UK to third-countries that are not deemed ensuring an adequate level of data protection (i.e. countries that have not been subject to an adequacy decision by the European Commission or that have qualified as adequacy regulation by the Information Commissioner's Office) , the Company ensures, in particular:

- Implementing the necessary safeguards to ensure an adequate level of data protection, in line with Article 46 GDPR. Those safeguards may include:
  - entering into Standard Contractual Clauses or international data transfer agreements issued by competent supervisory authorities (such as, as the case may be, the Standard Contractual Clauses issued by the European Commission ("**SCCs**") or the International transfer addendum to the EU SCCs ("**Addendum**") or the UK standalone international data transfer agreement ("**IDTA**").
  - seeking assurances from the recipients that they have Binding Corporate Rules in place; or
  - in exceptional circumstances, rely on a derogation under applicable data protection law (e.g., where the transfer is necessary for the defence of legal claims).
- That enforceable rights and effective legal remedies are available to the relevant data subjects.
- Having in place all the measures supplementing transfer tools to ensure compliance with the EEA/UK levels of personal data protection, in line with, as the case may be, the European Data Protection Board Recommendations 01/2020, as lastly amended in June 2021 and the guide to international transfers issued by the Information Commissioner's Office.

Marketing activities

The Company ensures that marketing communications are only issued to data subjects where each relevant data subject has previously consented to receive such marketing communications (i.e., via opt-in) and that the data subjects are always provided with the opportunity to opt-out/object (free of charge) when their personal data is collected as well as in all future communications.

Automated decision making and profiling

The Company ensures:

- Appropriately informing data subjects of profiling and/or automated decision making; and
- Enforcing the right of the data subject not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or significantly affects the data subject.

Data breach notifications

The Company ensures having all processes and procedures in place to:

- Notify to the competent data protection authority, without undue delay and no later than 72

hours after becoming aware of it, of any personal data breach that is likely to present a risk to the rights and freedoms of the relevant data subjects; and

- Communicate to the data subject, without undue delay, of any personal data breach that is likely to present a high risk to his/her/their rights and freedoms.

Monitoring

The DPO is responsible for monitoring this Policy. The DPO will ensure that all necessary improvements are undertaken to maintain the best mitigation of the risk related to data protection.

The review and maintenance of this Policy is an ongoing process that will depend on circumstances and potential one-time events. For example, changes in the regulatory framework applicable to the data protection.

In addition to ad hoc reviews, the DPO will be required to review the Policy annually.