Data Protection Policy

Contents

1. Introduction

Inet3 Ltd t/as magenta insurance needs to gather and use certain information about individuals (Data Subjects). These can include clients, customers, suppliers, employees and other individuals that magenta insurance has a relationship with or may need to contact. In doing so, magenta insurance is committed to complying with applicable Data Protection Laws and protecting the Data Protection rights of individuals.

This policy incorporates our Data Security Policy, Data Retention Policy & Subject Access Requests

2. Scope

The Data Protection Policy ("Policy") applies to all employees & contingent workers of magenta insurance. Disciplinary action may be taken against employees or contingent workers failing to comply with this Policy. Failing to comply with the provision of Data Protection legislation may result in legal action being taken against the individual and/or magenta insurance.

3. Purpose

The purpose of this Policy is to explain the Data Protection principles to be practiced and how Personal Data must be managed, taking into account the context within which magenta insurance operates and including the legal and regulatory environment, e.g., the UK GDPR (which merges the Data Protection Act 2018 and the UK's retained sections
of the environment, e.g., the UK GDPR (which merges the Data Protection Act 2018 and the UK's retained sections of the General Data Protection Regulation (Regulation (2016/679) (the EU GDPR), and other legal obligations.

For the purposes of the Policy, Personal Data also includes Special Category (sensitive) Personal Data.

Personal Data can be held on computers, laptops, iPads, tablets and mobile devices, or in a manual (hardcopy paper) file, and includes emails, telephone call recordings, minutes of meetings, CCTV recordings, audiovisual and photographs.

Benefits

The Policy ensures that magenta insurance:

- Complies with the UK GDPR, other associate legislation and best practice;
- Staff are aware of their responsibilities, and magenta insurance's expectations regarding data privacy and protection;
- Protects the rights of staff, clients, customers and partners;
- Is open about how it processes individual's personal data, which instills trust and confidence in individuals; and
- Protects individuals, and itself, from the risks of a Personal Data breach.

4. Review

The policy will be reviewed at least annually and all changes approved by the applicable DPO

5. Responsibilities

All employees and contingent workers are responsible for complying with the requirement of this Policy and any associated policies, procedures and guidance.

6. Principles for processing Personal Data

Data Protection is underpinned by seven important principles to guide how we should manage personal data

a. Lawfulness, Fairness and Transparency

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

b. Purpose Limitation

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

c. Data Minimization

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

d. Accuracy

Personal Data shall be accurate and, where necessary, kept up to date.

e. Storage Limitation

Personal Data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

f. Integrity and Confidentiality

Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

g. Accountability

magenta insurance shall be responsible for, and be able to demonstrate, compliance with the UK GDPR.

7. Lawfulness of Processing

A. Processing Personal Data

We will be lawfully processing Personal Data only if at least one of the following legal grounds applies:

Consent: The data subject has given their consent to the processing of their personal data for the specified purposes.
Contractual: Processing is necessary for the performance of a contract to which the data subject is part or in order to take steps at the request of the data subject prior to entering into a contract.
Legal Obligation: Processing is necessary for compliance with a legal obligation to which the magenta insurance is subject.
Vital Interests: Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
Public Task: Processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in magenta insurance.
Legitimate Interest: Processing is necessary for the purposes of legitimate interests of magenta insurance or a third party acting on our behalf (e.g., an external processor), except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child

B. Processing special category (sensitive) personal data

Magenta insurance will be lawfully processing special category (sensitive) personal data only if one or more of the following reasons are proven:

Substantial public interest: Processing is necessary for reasons of substantial public interest on the basis of UK law which is proportionate to the aim pursued and which contains appropriate safeguards. (This is the legal basis upon which magenta insurance process special category (sensitive) personal data1 for 'insurance purposes', subject to meeting certain criteria
Explicit consent: Explicit consent of the data subject has been obtained.
Legal obligation related to employment: It is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement.
Vital interests: It is necessary to protect the vital interests of a data subject or another person where the data subject is physically or legally incapable of giving consent.
Public information: Processing relates to personal data manifestly made public by the data subject.
Legal claims: Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
Healthcare: Processing is necessary for the purposes of medical treatment, for assessing the working capacity of employees or the provision, treatment or management of health or social care systems and services.
Public health: Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
Archive: Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes

C. Conditions for consent

Where processing of personal data is based on consent, we must be able to demonstrate that the data subject has given their consent to this processing. The following conditions must be followed:

- magenta insurance must be able to demonstrate that the Data Subject has provided consent
- Consent must be freely given, specific, informed and unambiguous
- Any request for consent must be presented in a manner which is clearly distinguishable from other matters
- Any request for consent must be in intelligible and easily accessible form, using clear and plain language
- Data Subject will have the right to withdraw consent at any time and must be told of that right when consent is sought
- It must be as easy to withdraw consent as it is to give consent
- The performance of a contract / provision of a service cannot be conditional on consent being given.

1 Except political opinions, biometric data for the purpose of uniquely identifying a natural person and data concerning a natural person's sex life or sexual orientation.
2 Processing must be necessary for a defined insurance purpose; processing must be necessary for reasons of substantial public interest (e.g., providing insurance, investigating fraudulent claims, claims management); the processing has been designed so that it affords additional safeguards to the data subject who does not have rights or obligations in respect of the insurance contract or insured person, and there is an insurance contact in place.

D. Processing children's personal data

Children (data subjects under 13 years) merit specific protection with regard to their personal data as they are less aware of the risks. We shall lawfully process a child's personal data only if at least one of the following legal grounds applies:

- Consent (person with parental responsibility, a legal guardian, Court appointed deputy, etc.)
- Necessary for the performance of a contract
- Legitimate interests.

Children have the same rights as adults over their personal data. These include the rights to access their personal data, request rectification, object to processing and have their personal data erased. A data subject's right to erasure is particularly relevant if consent was given for processing when they were a child.

E. Processing personal data relating to criminal convictions and offences

We will consider and treat personal data relating to a criminal convictions and offences as special category (sensitive) personal data for the purposes of processing the personal data

F. Processing not requiring identification

Where we are the data controller and the purposes for which we process personal data do not, or no longer require identification of the data subject, we are not obliged to maintain, acquire or process additional information in order to identify the data subject to comply with the UK GDPR. Where this occurs, we must inform the data subject of such. The data subject rights will not apply, except where the data subject provides additional information to enable their identification

G. Legitimate Interest Assessment (LIA)

Where appropriate, we will conduct a LIA to ensure the processing meets the threshold required to rely on legitimate interests as a lawful basis. Further information is provided in the Legitimate Interests Assessment (LIA) Guide

8. Internal personal data

This policy and associated policies, procedures and guidance also applies to internal personal data, such as the personal data of employees/ex-employees and their partners/dependents/benefactors and contingent workers

9. Data subject rights and requests

A. Data subject rights (in accordance with Chapter 3, Section 2 of the UK GDPR)

Data subjects have the right to:

- Be informed
- Gain access to their personal data
- Rectify their personal data
- Erasure of their personal data (also known as the 'right to be forgotten')
- Restrict the processing of their personal data
- Data portability
- Object to the processing of their personal data
- Not be subject to automated decision-making (or profiling)

Further information on data subject rights is provided in the Data Subject Rights Policy and Procedure

B. Data subject rights requests

Data subject rights requests can be received directly from the data subject or a third party acting on the data subject's behalf, e.g., solicitor, person with parental or legal responsibility, or simply someone acting on the data subject's

behalf. Information on the process to be followed when responding to a data subject rights requests is provided in the Data Subject Rights Policy and Procedure.

10. Personal Data breaches

We may need to report certain types of personal data breach to the ICO within 72 hours of becoming aware of the breach (where feasible), and where the breach results in a risk to the rights and freedoms of data subjects. If the breach is likely to result in a high risk of adversely affecting data subject's rights and freedoms, we may also be required to inform the affected data subjects without due delay. A record of any personal data breaches, regardless of whether we are required to notify, must be kept. Information on the process to be followed in the event of a personal data breach is provided in the Personal Data Breach Policy.

11. Data sharing and transfer

The sharing and transfer of personal data must be based upon at least one of the lawful basis provided in the UK GDPR.

We shall ensure that formal agreements are in place with all our data processors and sub-processors and comply with the requirements of Article 28 of the UK GDPR. Where necessary, legal advice will be the obtained. Agreements must be regularly reviewed to verify that there is still a lawful basis for data sharing.

Additional measures, such as the safeguards to protect the personal data, must be put in place to ensure the lawful transfer of data to a country which the UK Secretary of State does not consider has an adequate level of protection for the rights of data subjects. These safeguards can include agreements containing the applicable and approved Standard Contractual Clauses.

The sharing and transfer of personal data within Magenta insurance and its subsidiaries is supported by an Intra-Group Data Sharing Agreement, as well as an Inter-company Agreement (ICA) for where data is shared with UK-based Magenta insurance subsidiaries for statistical analysis and other data analytical activities.

Where any Personal Data is to be transferred outside of the UK, the Group Data Protection Officer must be engaged to provide support and guidance

12. Storage

a. Retaining, archiving and disposing of records containing personal data

We will ensure that all our records that contain personal data are stored appropriately, accessible and easily traced and retained in line with our Data Retention policy.

b. Security of stored personal data

We shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted (shared or transferred), stored or otherwise processed. Further information on the security of personal information is provided in the Information Security Policy

13. Privacy by design

We shall ensure that appropriate technical and organisational measures are in place for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. Where relevant, we will conduct data privacy impact assessments (DPIA) to ensure that all personal data collection, processing, storage and destruction measures are designed to secure privacy. Where the DPIA indicates that the processing would result in a high residual risk, after taking measures or where no further measures are able to be taken to mitigate the risk, we must consult with the Information Commissioner's Office (ICO) prior to starting the processing.

14.Records of processing activities

We will keep a record of our processing activities in relation to personal data under our responsibility as a data controller and a data processor.

15.Training

We will ensure that appropriate training is provided to all employees and contingent workers managing and handling personal data to ensure they are familiar with and understand that they must follow the data privacy and protection principles.

16.Co-operation with the Information Commissioner's Office

We will co-operate, on request, with the ICO in the performance of its tasks.

17. Local Data Security Officer Contact

Contact: Matthew Taylor 3, Whiting Street, Bury St Edmunds, Suffolk. IP33 1NX
03300 555 210; data@magentainsurance.co.uk

18.Glossary

Key Term	Definition
Anonymise, anonymised, anonymising	The process of rendering data into a form which does not identify individuals and where identification is not likely to take place. Anonymised data is data that is in a form that does not identify individuals and where identification through its combination with other data is not likely to take place. A copy of the 'Anonymisation Code of Practice' is on the ICO website
Automated decision making	It relates to having the ability to make decisions by technological means without human intervention. For automated decision making: • there must be a decision • there must be automated processing, which may include profiling • the decision must be based solely on automated decision making • the decision must produce legal effects or otherwise significantly affect the data subject. Automated individual decision-making does not have to involve profiling, although it often will do
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or fingerprints.
Child	A data subject under the age of 13 years
Consent	'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.
Contingent worker	Contingent workers are defined as freelancers, independent contractors, consultants, or other outsourced and non-permanent workers who are hired on a per-project basis. They can work on site or remotely
Data concerning health	Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status
Controller	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.
Processor	A natural or legal person, public authority, agency, organisation or other body that processes personal data on behalf of magenta insurance. magenta insurance is a data processor, where it processes data on behalf of a data controller.

Data sharing	Data sharing is the disclosure of data from one or more organisations to a third-party organisation or organisations, or the sharing of data between different parts of an organisation. Data sharing can take the form of: • a reciprocal exchange of data; • providing data to a third party or parties; • organisations pooling information and making it available to each other, or to a third party(ies); • exceptional, one-off disclosures of data in unexpected or emergency situations; or • sharing data within magenta insurance. The UK GDPR does not apply to data sharing where it doesn't involve personal data, .e.g., where statistics that cannot identify individuals is shared.
Data subject	A natural person (i.e., one who has its own legal personality) that is an individual human being, as opposed to a legal person, which may be a private (i.e., business entity or non-governmental organisation) or public (i.e., government) organisation.
Employee	An individual who works part-time or full-time for magenta insurance under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. Includes temporary employees and independent contractors
Genetic data	Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that Page | 12 HYPERION Key Term Definition natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
Personal data	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
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.
Process, Processed, Processing	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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling has to involve some form of automated processing of personal data and can be part of an automated decision making process. Profiling could be simply assessing or classifying individuals based on characteristics such as their age, sex and height, regardless of any predictive process. As such, profiling is not in or of itself an automated decision
Pseudonymise, pseudonymized, pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person
Special catagory (sensitive) personal data, Sensitive personal data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation
Statistical data	Information which is held in the form of numerical data, nominal data (e.g., gender, ethnicity, region), ordinal data (age group, qualification level), interval data (month of birth) or ratio data (age in months).

Third Party	A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data