Data Protection Policy

Version 0.3

Version Control

	Last Amended	Author	Action taken
0.1	15/11/2018	Loren Morrison	Document created
0.2	01/11/2019	Loren Morrison	Reviewed – no amends
0.3	01/11/2020	Kas Khalil	Reviewed – no changes however a further review will be required after Brexit to bring in line with UK-GDPR

Contents

Version Control **2**

Contents **3**

Purpose **4**

Scope **4**

Objectives **4**

Data Protection Policy Statement **5**

Transmitting Personal Data *5*
Storing Personal Data *5*
Breaches of Personal Data *5*
Subject Access Request (SAR) *5*
Responsibilities *6*

Definitions **6**

Data *6*
Processing *6*
Data Subject *7*
Data Controller *7*
Data Processor *7*
Personal Data *7*
Sensitive Data *7*

This Policy **7**

Purpose

The purpose of this policy is to ensure that Preferred Management and its staff (meaning permanent, fixed term, and temporary staff, any third party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with Preferred Management, conduct their business practices in a manner compliant with the Data Protection Act 1998 ("DPA") and the General Data Protection Regulations (GDPR:2018) and its principles to ensure that all Personally Identifiable Information (PII) is secure, accurate and up-to-date at all times.

Scope

This policy applies to all members of the organisation and those contracted to work on behalf of Preferred Management and is to be followed at all times. Its aim is to protect the rights of individuals and applies to all personal and sensitive information that is used, stored and transmitted either electronically or via paper-based methods.

Objectives

The objective of this policy is to protect the rights of individuals with regards to the personal information known and held about them by Preferred Management in the course of business and ensure that every business practice, task and process carried out by Preferred Management is compliant with each principle of the Data Protection Act 1998 and the General Data Protection Regulation (GDPR:2018)

Preferred Management aim to ensure that staff are trained and aware of the guiding principles behind Data Protection of PII, namely to ensure;

- **Confidentiality** – That PII will be handled with due regard to its sensitivity and appropriate security measures put in place to maintain its confidentiality
- **Integrity** – That the PII which is held by Preferred Management is up to date, accurate and can be relied upon.
- **Availability** – That the PII will be available to the data subject upon request (as per their 'Subject Access Rights')

This policy is therefore in place to ensure regulatory and legal compliance at all times with regards to handling and processing personal data.

Data Protection Policy Statement

Preferred Management is classed as a Data Controller/Data Processor under the current Data Protection Act 1998, however Preferred Management recognises that under the new General Data Protection Regulations (GDPR:2018) our obligations to ensure appropriate controls are in place irrespective of classification is of critical importance.

This policy confirms our commitment to protect the privacy of PII of our customers, clients, employees and other interested parties. Preferred Management have engaged in a programme of Information Security Management which is aligned to the international standard, ISO27001:2013 to ensure that the processes of personal information is conducted using best practice processes.

The following sections, detail Preferred Management practices which are directly linked to Data Protection requirements, and are supported by further policies and procedures which can be requested by data subjects.

Transmitting Personal Data

Where personal data is to be transmitted (either electronically or in hard copy), staff are required to ensure that any such data is secured using appropriate measures (e.g. Use of encryption, passwords for electronic transmissions or using secure couriers).

Personal Data will only be transmitted in accordance with best practice and processes noted as part of the ISMS.

Personal data is only transmitted to a person authorised to receive it in compliance with these Data Protection principles.

Storing Personal Data

Personal data in hard copies (e.g. paper medical records, copy passport etc) are retained only for as long as is essential to the account and/or customer, employee or other interested party that they refer to.

Personal data in hard copy or electronic formats will be stored in accordance with best practice and inline with processes, which are part of a broader Information Security Management System (ISMS).

The management of Personal Data is controlled through this standard and Preferred Management have committed to ongoing audit and review of policies, processes and practices associated to holding information in all its form.

Breaches of Personal Data

If any breach of the DPA or its Principles occurs, staff are required to inform their line manager, who will report the details to the Head of Operations / Operations Director, to be logged and investigated, in line with Preferred Management Incident Management processes.

Upon notification and initial Preferred Management will ensure that when deemed necessary, both the Information Commissioners Office and the data subjects affected will be informed without undue delay.

Subject Access Request (SAR)

An individual has the right to see what personal information is being held about them by Preferred Management If an individual makes a written request to us and asks for information under the Subject Access Request provisions, they are entitled to request:

- information on whether any personal data is being processed;
- what personal information is being held by Preferred Management;
- a description of the personal data, the reason it is being processed and whether it is shared with third-parties (and know who they are);

- details of the source of the data

Where any Subject Access Request is received Preferred Management will not charge for such a request and will work with the individual making the request to understand what the nature of the request is and provide this information within one month of the request being made.

Responsibilities

Preferred Management recognises it has a responsibility to ensure that PII is protected using appropriate technical and operational measures and as such has implemented a security framework which focuses on both operational and technical aspects of data protection. In this regard Preferred Management have;

- Implemented controls to ensure that staff cannot gain access to information that is not necessary for them to carry out their job functions.
- Put in place measures to ensure that all information held will be relevant, accurate and up-to-date and used only for the purpose for which it is required and was originally intended.
- Committed to ensure information will not be kept for longer than is necessary and will be kept secure at all times.

Preferred Management staff who manage and process personal or sensitive personal information will ensure that it is kept secure and sensitive personal information will only be processed fairly and lawfully and in line with the provisions set out in relevant Data Protection regulations.

Preferred Management will ensure that all staff are made aware of the reasons why personal and sensitive personal data is being processed and are provided with frequent and ongoing training and support with regards to Data Protection.

Definitions

To ensure Preferred Management understands its obligations to the protection of PII, the following definitions apply and are based on current understanding of these terms within UK and European law.

Data

'Data' means information which;

a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

b) is recorded with the intention that it should be processed by means of such equipment,

c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68 Data Protection Act 1998, or

e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

Processing

'Processing', in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including;

a) organisation, adaptation or alteration of the information or data,

b) retrieval, consultation or use of the information or data,

c) disclosure of the information or data by transmission, dissemination or otherwise making available, or,

d) alignment, combination, blocking, erasure or destruction of the information or data.

Data Subject
Data Subject refers to a living individual who is the subject of Personal Data.

Data Controller
The ‘Data Controller’ is, a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any Personal Data are, or are to be, processed.

Data Processor
The ‘Data Processor’, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the Data Controller.

Personal Data
‘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.

Sensitive Data
‘Sensitive Personal Data’ means data which relates to a living individuals’;

a) Sexual orientation
b) Religion
c) Trade union membership
d) Proceedings for any offence committed or alleged
e) Race
f) Political beliefs
g) Medical information

Sensitive Personal Data can only be recorded with the expressed permission from the individual to whom it relates.

This Policy

This document is subject to ongoing review as part of the annual review cycle and is signed off, annually by the Head of Operations / Operations Director of Preferred Management, who is ultimately accountable for Information Security at Preferred Management.