Data protection policy

As of the 25th May 2018, the EU General Data Protection Regulation (GDPR) was enacted into United Kingdom law as the Data Protection Act 2018 (referenced in this policy as UK DPA 2018 for the purposes of brevity). This Act superseded the preceding UK Data Protection Act 1998. The Data Protection Act 2018 incorporates all major elements of the GDPR with some allowed national modifications for law enforcement and national security purposes.

Although the UK has left the EU, there is a six month extension in place covering UK-EU and EU-UK data transfers, while the EU decides on an adequacy status for the UK as a third country and the UK determines its own adequacy decisions. The current expectation is that the UK will not deviate immediately from GDPR, as there is a strong desire from both sides for a continued free flow of data in line with the status quo ante.

For the purposes of any UK data protection policy produced after 25th May 2018, the UK DPA 2018 should be the legal point of reference, as any complaint to the Information Commissioners Office in the UK would be made against the provisions of that act. The EU GDPR articles and chapters can, however, continue to be quoted in such data protection, until such time as any fundamental changes are made to the UK Data Protection Act 2018.

1. POLICY STATEMENT

1.1 Kindred LCR CIC ("the Company") is committed to comply with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information the Company collects and processes in accordance with the General Data Protection Regulation (GDPR) enacted into UK law as the Data Protection Act 2018 (UK DPA 2018).

1.2 The Company insists that all employees and Board members recognise the significance of dealing with such information, including the many risks that are involved.

1.3 Any breach of this policy or the UK DPA 2018 will be dealt with under the Company's Disciplinary policy. In the case where a breach also constitutes a criminal offence, the matter will be reported to the appropriate authorities as soon as possible.

2. POLICY OBJECTIVES

2.1 To ensure compliance with data protection laws and generally with good practice

2.2 To outline how personal data should be processed in accordance with data subject's rights.

2.3 To protect the Company from risks of data breaches.

3. DEFINITIONS AND TYPES

3.1 Material Scope – the applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

3.2 Territorial Scope - the GDPR (as incorporated into the UK DPA 2018) will apply to all controllers that are established in the:

EU (European Union) - who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour of data subjects who are resident in the EU.

UK (United Kingdom) – since the departure of the UK from the EU, all existing definitions will be maintained under a transition equivalence arrangement in place for at least six months from 1st January 2021. It appears unlikely that the UK will depart dramatically from the GDPR articles at this time.

DEFINITIONS FROM ARTICLE 4 OF THE GDPR as incorporated into the UK DPA 2018:

3.3 Establishment - the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

3.4 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.

3.5 Special categories of personal data - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of 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.

3.6 Data 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; 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.

3.7 Data subject - any living individual who is the subject of personal data held by an organisation.

3.8 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.

3.9 Profiling - is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

3.10 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. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

3.11 Data subject consent - 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.

3.12 Child - the GDPR as incorporated into the UK DPA 2018 defines a child as anyone under the age of 16 years old,

although this may be lowered to 13 by Member State law. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

3.13 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.

3.14 Filing system - any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

4. SCOPE

4.1 This policy and procedure covers the Company as a whole.

4.2 The rights and obligations set out in this policy and procedure applies to employees and Board members of the Company.

4.3 The GDPR and this policy apply to all of the Company's personal data processing functions including those performed on clients', employees', Board members', suppliers', partners' personal data and any other personal data the organisation processes from any source.

5. DUTIES – ROLES AND RESPONSIBILITIES

5.1 The Board of Directors have the ultimate responsibility to provide, implement and review this policy.

5.2 The Data Protection Officer/Owner is responsible for assisting the Company in monitoring internal compliance, informing and advising members and employees on their data protection obligations, providing advice regarding Data Protection Impact Assessments (DPIAs) and acting as a contact point for data subjects and the supervisory authority.

6. PRINCIPLES AND RIGHTS

Data Protection Principles

6.1.1 All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR as incorporated into the UK DPA 2018. The Company's policy and procedure are designed to ensure compliance with the principles.

6.1.2 Personal data must be processed lawfully, fairly and transparently.

- Lawfully - identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing".

What are the lawful bases for processing

- The lawful bases for processing are set out in Article 6 of the GDPR as incorporated into the UK DPA 2018. At least one of these must apply whenever you process personal data:

i. Consent : The individual has given clear consent for you to process their personal data for a specific purpose.

ii. Contract : the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract

iii. Legal obligation : the processing is necessary for you to comply with the law (not including contractual obligations)

iv. Vital interests : the processing is necessary to protect someone's life

v. Public task : the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law

vi. Legitimate interests ; the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is good reason to protect the individual's personal data which overrides those personal interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

- Fairly - in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

- Transparently - the GDPR as incorporated into the UK DPA 2018 includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

6.1.3 The specific information that must be provided to the data subject must, as a

minimum, include:

- The identity and the contact details of the controller and, if any, of the controller's representative;

- The contact details of the Data Protection Officer/Owner;

- The purposes of the processing for which the personal data are intended as well as the legal basis for processing:

- The period for which the personal data will be stored;

- The existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected

- The categories of personal data concerned;

- The recipients or categories of recipients of the personal data where applicable;

- Where applicable, that the controller intends to transfer personal data to a recipient in a third country, and the level of protection afforded to that data and any further information necessary to guarantee fair processing

6.1.4 Personal data can only be collected for specific, explicit and legitimate purposes.

• Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of the Company's GDPR register of processing.

6.1.5 Personal data must be adequate, relevant and limited to what is necessary for

processing.

• The Data Protection Officer/Owner is responsible for ensuring that the Company does not collect information that is not strictly necessary for the purpose for which it is obtained

• All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to privacy statement and approved by the Data Protection Officer.

• The Data Protection Officer/Owner will ensure that, on a 12-monthly basis all data collection methods are reviewed by internal audit to ensure that collected data continues to be adequate, relevant and not excessive.

6.1.6 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay:

• Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

• The Data Protection Officer/Owner is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

• It is also the responsibility of the data subject to ensure that data held by the Company is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

• Employees/Staff should be required to notify the Company of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the Company to ensure that any notification regarding change of circumstances is recorded and acted upon.

• The Data Protection Officer/Owner is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

• On at least a 12-monthly basis, the Data Protection Officer/Owner will review the retention dates of all the personal data processed by the Company, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the agreed procedures and in line with recommended practice.

• The Data Protection Officer/Owner is responsible for responding to requests for rectification from data subjects within one month, in line with the Subject Access Request Procedure. This can be extended to a further two months for complex requests. If the Company decides not to comply with the request, the Data Protection Officer/Owner must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

• The Data Protection Officer/Owner is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them

that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

6.1.7 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

- Where personal data is retained beyond the processing date, it will be minimised appropriately in order to protect the identity of the data subject in the event of a data breach.

- Personal data will be retained in line with the Retention of Records Procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

- The Data Protection Officer/Owner must specifically approve any data retention that exceeds the retention periods defined in Retention of Records Procedure and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

6.1.8 Personal data must be processed in a manner that ensures the appropriate security.

- The Data Protection Officer/Owner will carry out a risk assessment taking into account all the circumstances of the Company's controlling or processing operations.

- In determining appropriateness, the Data Protection Officer/Owner should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on the Company itself, and any likely reputational damage including the possible loss of member or stakeholder trust.

At a point that Kindred have an established physical organisation with technical infrastructure, the Data Protection Officer/Owner will consider the following:

- Password protection

- automatic locking of idle screens

- removal of access rights for USB and other memory

- virus checking software and firewalls

- role-based access rights including those assigned to temporary staff

- encryption of devices the leave the organisations premises such as laptops

- security of local and wide area networks

- privacy enhancing technologies such as pseudonymisation and anonymisation

- identifying appropriate international security standards relevant to Kindred

When assessing appropriate organisational measures, including during the initial startup period, the Data Protection Officer/Owner will consider the following:

- the appropriate training levels throughout Kindred

- measures that consider the reliability of employees (such as references etc)
- the inclusion of data protection in employment contracts
- identification of disciplinary action measures for data breaches
- monitoring of staff for compliance with relevant security standards
- use of a code of conduct to establish acceptable data access and management approaches
- physical access controls to electronic and paper-based records, as well as the minimising of duplication
- adopting clear rules about passwords
- making regular backups of personal data and storing the media off site
- the imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside of the UK or EEA

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

6.1.9 The controller must be able to demonstrate compliance with the GDPR's other principles (accountability).

- The GDPR as incorporated in the UK DPA 2018 includes provisions that promote accountability and governance. These complement the Regulation/Act's transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.
- The Company will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans as needed.

DATA SUBJECTS' RIGHTS

Data subjects have the following rights regarding data processing and the data that is recorded about them

- to make subject access requests regarding the nature of information held and to whom it has been disclosed
- to prevent processing likely to cause damage or distress
- to prevent processing for purposes of direct marketing
- to be informed about the mechanics of automated decision-taking processes that will affect them
- to not have significant decisions that will affect them taken solely by automated process
- to sue for compensation if they suffer damage by any contravention of the GDPR

- to take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data
- to request the supervisory authority to assess whether any provision of the GDPR has been contravened
- to have personal data provided to them in structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller
- to object to any automated profiling that is occurring without consent

6.2.1 The Company will ensure that data subjects may exercise these rights:

- Data subjects may make data access requests as described in Subject Access Request Procedure this procedure also describes how the Company will ensure that its response to the data access request complies with the requirements of the GDPR.
- Data subjects have the right to complain to the Company related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Complaints Procedure.

7. PROCEDURES

The Company will process all Member and Employee data in accordance with the Member and Employee Privacy Notices in force from time to time, copies of which are provided to all Members and Employees and which appear on the Company's website, and for which the Data Protection Officer/Owner is responsible.

This policy has been approved and authorised by:

Name: Kindred Interim Board

Position: X

Date: 15/06/2021

Policy Name	Version	Developed by	Amended y/n	Review Date
Data Protection Pollicy	1	DC	n/a	15/06/22