# Data Protection Policy

## 1. Introduction

1.1 Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data (including photos and videos) are not processed without their knowledge, and, wherever possible, that it is processed with their consent.

1.2 Definitions used by the organisation (drawn from the GDPR)

Material scope (Article 2) – the GDPR 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.

Territorial scope (Article 3) – the GDPR 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 behavior of data subjects who are resident in the EU.

1.3 Article 4 definitions

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.

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 also includes photos and videos.

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.

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.

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

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 – 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 behavior. 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.

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.

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.

Child – the GDPR 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.

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.

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.

## 2. Policy statement

2.1 HorseHeard, located at Malvern House is committed to compliance 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 Organisation Name collects and processes in accordance with the General Data Protection Regulation (GDPR).

2.2 Compliance with the GDPR is described by this policy and other relevant policies such as the Information Security Policy along with connected processes and procedures.

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

2.4 Data Protection Officer/GDPR Owner is responsible for reviewing the register of processing annually in the light of any changes to HorseHeard's activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments. This register needs to be available on the supervisory authority's request.

2.5 Partners and any third parties working with or for HorseHeard, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by HorseHeard without having first entered into a data confidentiality agreement, which imposes on the third party obligations no less onerous than those to which HorseHeard is committed, and which gives HorseHeard the right to audit compliance with the agreement.

## 3. Responsibilities and roles under the General Data Protection Regulation

HorseHeard is a data controller under the GDPR. Those in managerial or supervisory roles throughout HorseHeard are responsible for developing and encouraging good information handling practices within HorseHeard.

3.1 Data Protection Officer (DPO), a role specified in the GDPR, should be a member of the senior management team and have appropriate authority, is accountable to the CEO for the management of personal data within the organisation and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

3.1.1 development and implementation of the GDPR as required by this policy; and
3.1.2 security and risk management in relation to compliance with the policy.

3.2 A Data Protection Officer, who the CEO and Trustees considers to be suitably qualified and experienced, has been appointed to take responsibility for HorseHeard's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that HorseHeard complies with the GDPR, as do the management team in respect of data processing that takes place within their area of responsibility.

3.3 The Data Protection Officer has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and is the first point of call for clarification on any aspect of data protection compliance.

3.4 Compliance with data protection legislation is the responsibility of all involved in HorseHeard who process personal data.

3.5 Management, Trustees and Facilitators of HorseHeard are responsible for ensuring that any personal data about them and supplied by them to HorseHeard is accurate and up-to-date.

## 4. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. HorseHeard's policies and procedures are designed to ensure compliance with the principles.

4.1 <u>Personal data must be processed lawfully, fairly and transparently</u>
Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

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.

The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

Transparently – the GDPR 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.

The specific information that must be provided to the data subject must, as a minimum, include:

4.1.1 the identity and the contact details of the controller and, if any, of the controller's representative;
4.1.2 the contact details of the Data Protection Officer;
4.1.3 the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4.1.4 the period for which the personal data will be stored;

4.1.5 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;

4.1.6 the categories of personal data concerned;

4.1.7 the recipients or categories of recipients of the personal data, where applicable;

4.1.8 where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;

4.1.9 any further information necessary to guarantee fair processing.

4.2 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 HorseHeard's GDPR register of processing and as explained in the Privacy Procedure

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

4.3.1 The Data Protection Officer is responsible for ensuring that HorseHeard does not collect information that is not strictly necessary for the purpose for which it is obtained.

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

4.3.3 The Data Protection Officer will ensure that, on an as appropriate basis all data collection methods are reviewed by internal audit/external auditors to ensure that collected data continues to be adequate, relevant and not excessive.

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

4.4.1 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.

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

4.4.3 It is also the responsibility of the data subject to ensure that data held by HorseHeard 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.

4.4.4 The Data Protection Officer 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.

4.4.5 On at least an annual basis, the Data Protection Officer / GDPR Owner will review the retention dates of all the personal data processed by HorseHeard, 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 Secure Disposal of Storage Media Procedure.

4.4.6 The Data Protection Officer is responsible for responding to requests for rectification from data subjects within one month (Subject Access Request Procedure). This can be extended to a further two months for complex requests. If HorseHeard decides not to comply with the request, the Data Protection Officer 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.

4.4.7 The Data Protection Officer 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.

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

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

4.5.2 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.

4.5.3 The Data protection Officer 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.

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

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

In determining appropriateness, the Data Protection Officer 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 HorseHeard itself, and any likely reputational damage including the possible loss of customer trust.

When assessing appropriate organisational measures the Data Protection Officer will consider the following:

- The appropriate training levels throughout HorseHeard.
- Storing of paper based data in lockable fire-proof cabinets;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;

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

The GDPR includes provisions that promote accountability and governance. These complement the GDPR'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.

HorseHeard 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.

## 5. Data subjects' rights

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

5.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.

5.1.2 To prevent processing likely to cause damage or distress.

5.1.3 To prevent processing for purposes of direct marketing.

5.1.4 To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.

5.1.5 To request the supervisory authority to assess whether any provision of the GDPR has been contravened.

5.1.6 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

## 6. Consent

6.1 HorseHeard understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

6.2 HorseHeard understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them.

6.3 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation and record kept of this.

6.4 In most instances, consent to process personal and sensitive data is obtained routinely by HorseHeard using standard consent documents. e.g. when a new client signs a contract, or during induction for participants on programmes.

## 7. Security of data

7.1 All Management, Trustees and Facilitators are responsible for ensuring that any personal data that HorseHeard holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by HorseHeard to receive that information and has entered into a confidentiality agreement.

7.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. All personal data should be treated with the highest security and must be kept:

- in a locked drawer or filing cabinet; and/or
- if computerised, password protected
- stored on (removable) computer media which are encrypted in line with Secure Disposal of Storage Media

7.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised individuals.

7.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit written authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with the HorseHeard data retention guidelines.

- Personal data may only be deleted or disposed of in line with the Retention of Records Procedure as 'confidential waste'.
- Hard drives of redundant PCs are to be removed and immediately destroyed or as disposed of in line with Secure Disposal of Storage Media

## 8. Disclosure of data

8.1 HorseHeard must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All authorised individuals should exercise caution when asked to disclose personal data held on another individual to a third party. Staff should seek advice from the Data Protection Officer if there is any concern

8.2 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer

## 9. Retention and disposal of data

9.1 HorseHeard shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

9.2 The retention period for each category of personal data will be set out in the Retention of Records Procedure) along with the criteria used to determine this period including any statutory obligations HorseHeard has to retain the data.

9.3 HorseHeard data retention and data disposal procedures will apply in all cases.

9.4 Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure

## 10. Information asset register/data inventory

10.1 HorseHeard has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project. HorseHeard data inventory and data flow determines

- business processes that use personal data;
- source of personal data;
- volume of data subjects;
- description of each item of personal data;
- processing activity;
- maintains the inventory of data categories of personal data processed;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of the Organisation Name throughout the data flow;
- key systems and repositories;
- all retention and disposal requirements.

10.2 HorseHeard is aware of any risks associated with the processing of particular types of personal data and makes the appropriate assessment such as DPIA.

***Document Owner and Approval***

The Data Protection Officer / GDPR Owner is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff after training or on document change

This policy was approved by the CEO on 30/03/2018 and is issued on a version controlled basis.

Signature: Date:

**Change History Record**

| Issue | Description of Change | Approval | Date of Issue |
|---|---|---|---|
| 1 | Initial issue | | |
| 2 | Clarification of wording and logo | H Hardy CEO | 30th March 2018 |
| 3 | Definition of personal data on page 1 also includes photos and videos | K. Smith | 4th April 2018 |