The Federation of Horses in Education and Therapy International

General Data Protection Regulation Policy

March 2022

Table of Contents

HETI's Data Protection Policy……3

HETI's Data loss notification Policy……10

HETI's Record Retention Policy……12

HETI's Data Protection Policy

Introduction

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of HETI. This includes obligations in dealing with personal data, in order to ensure that the organisation complies with the requirements of the relevant Irish legislation, namely the Irish Data Protection Act (1988), and the Irish Data Protection (Amendment) Act (2003).Since the HETI head office is currently in Ireland, Irish legislation has been adopted.

Rationale

HETI must comply with the Data Protection principles set out in the relevant legislation. This Policy applies to all Personal Data collected, processed and stored by HETI in relation to its staff, board members and clients in the course of its activities. HETI makes no distinction between the rights of Data Subjects who are employees, and those who are not. All are treated equally under this Policy.

Scope

The policy covers both personal and sensitive personal data held in relation to data subjects by HETI. The policy applies equally to personal data held in manual and automated form.

All Personal and Sensitive Personal Data will be treated with equal care by HETI. Both categories will be equally referred-to as Personal Data in this policy, unless specifically stated otherwise.

This policy should be read in conjunction with the associated Subject Access Request procedure, the Data Retention and Destruction Policy, the Data Retention Periods List and the Data Loss Notification procedure.

HETI as a Data Controller

In the course of its daily organisational activities, HETI acquires, processes and stores personal data in relation to:

- Federation Members of HETI
- Business Members of HETI
- Associate members of HETI
- Institute Members if HETI
- The Irish Register of Equine Assisted Activity Practitioners
- Human Equine Interaction Register
- Executive Committee/Board Members of HETI
- Employees of HETI
- Third party service providers engaged by HETI

In accordance with the Irish Data Protection legislation, this data must be acquired and managed fairly. Not all staff or board members will be expected to be experts in Data Protection legislation. However, HETI is committed to ensuring that its staff and board members/executive committee have sufficient awareness of the legislation in order to be able to anticipate and identify a Data Protection issue, should one arise. In such circumstances, staff and /or Board members/executive committee must ensure that the Data Protection Officer is informed, and in order that appropriate corrective action is taken.

Due to the nature of the services provided by HETI, there is regular and active exchange of personal data between HETI and its members. In addition, HETI exchanges personal data with Data Processors on the members' behalf.

This is consistent with HETI's obligations under the terms of its contract with its Data Processors.

This policy provides the guidelines for this exchange of information, as well as the procedure to follow in the event that a HETI staff member/board member is unsure whether such data can be disclosed.

In general terms, the staff member/board member should consult with the Data Protection Officer to seek clarification.

Subject Access Requests

Any formal, written request by a HETI member for a copy of their personal data (a Subject Access Request) will be referred, as soon as possible, to the Data Protection Officer, and will be processed as soon as possible.

It is intended that by complying with these guidelines, HETI will adhere to best practice regarding the applicable Data Protection legislation.

Third-Party processors

In the course of its role as Data Controller, HETI engages a number of Data Processors to process Personal Data on its behalf. In each case, a formal, written contract is in place with the Processor, outlining their obligations in relation to the Personal Data, the specific purpose or purposes for which they are engaged, and the understanding that they will process the data in compliance with the Irish Data Protection legislation.

These Data Processors include:

- Book keeper
- Accountant
- Website Designer

The Data Protection Principles

The following key principles are enshrined in the Irish legislation and are fundamental to the HETI's Data Protection policy.

In its capacity as Data Controller, HETI ensures that all data shall:

1. ... be obtained and processed fairly and lawfully.

For data to be obtained fairly, the data subject will, at the time the data are being collected, be made aware of:

- The identity of the Data Controller, HETI
- The purpose(s) for which the data is being collected
- The person(s) to whom the data may be disclosed by the Data Controller
- Any other information that is necessary so that the processing may be fair.

HETI will meet this obligation in the following way.

- Where possible, the informed consent of the Data Subject (to be called Member/Registrant herein) will be sought before their data is processed;
- Where it is not possible to seek consent, HETI will ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.;
- Processing of the personal data will be carried out only as part of HETI's lawful activities, and HETI will safeguard the rights and freedoms of the member/registrant;
- The Member/registrant's data will be disclosed to a third party other than to a party contracted to HETI and operating on its behalf.

2. .... be obtained only for one or more specified, legitimate purposes.

HETI will obtain data for purposes which are specific, lawful and clearly stated. A member/registrant will have the right to question the purpose(s) for which HETI holds their data, and HETI will be able to clearly state that purpose or purposes.

3. ..... not be further processed in a manner incompatible with the specified purpose(s).

Any use of the data by HETI will be compatible with the purposes for which the data was acquired.

4. .... be kept safe and secure.

HETI will employ high standards of security in order to protect the personal data under its care. Appropriate security measures will be taken to protect against unauthorised access to, or alteration, destruction or disclosure of any personal data held by HETI in its capacity as Data Controller.

Access to and management of staff and member/registrants's records is limited to those staff members who have appropriate authorisation and password access.

5. ... be kept accurate, complete and up-to-date where necessary.

HETI will:

- ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy;
- conduct periodic reviews and audits to ensure that relevant data is kept accurate and up-to-date. HETI conducts a review of sample data every six months to ensure accuracy; Member/registrant contact details are reviewed and updated every year.
- conduct regular assessments in order to establish the need to keep certain Personal Data.

6. ***... be adequate, relevant and not excessive in relation to the purpose(s) for which the data were collected and processed.***

HETI will ensure that the data it processes in relation to members are relevant to the purposes for which those data are collected. Data which are not relevant to such processing will not be acquired or maintained.

7. ***... not be kept for longer than is necessary to satisfy the specified purpose(s).***

HETI has identified an extensive matrix of data categories, with reference to the appropriate data retention period for each category. The matrix applies to data in both a manual and automated format. (see HETI's Record Retention and Destruction Policy)

Once the respective retention period has elapsed, HETI undertakes to destroy, erase or otherwise put this data beyond use.

8. ***... be managed and stored in such a manner that, in the event a member submits a valid Subject Access Request seeking a copy of their Personal Data, this data can be readily retrieved and provided to them.***

HETI has implemented a Subject Access Request procedure by which to manage such requests in an efficient and timely manner, within the timelines stipulated in the legislation.

Data Subject Access Requests

As part of the day-to-day operation of the organisation, HETI's staff/board members engage in active and regular exchanges of information with members. Where a formal request is submitted by a member/registrant in relation to the data held by HETI, such a request gives rise to access rights in favour of the member/registrant.

There are specific time-lines within which HETI must respond to the member/registrant, depending on the nature and extent of the request. These are outlined in the attached Subject Access Request process document.

HETI's staff will ensure that, where necessary, such requests are forwarded to the Data Protection Officer in a timely manner, and they are processed as quickly and efficiently as possible, but within not more than 40 days from receipt of the request.

Implementation

As a Data Controller, HETI ensures that any entity which processes Personal Data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection legislation.

Failure of a Data Processor to manage HETI's data in a compliant manner will be viewed as a breach of contract, and will be pursued through the courts.

Failure of HETI's staff /Board Member to process Personal Data in compliance with this policy may result in disciplinary proceedings.

This Policy was approved by the Board of Directors of HETI on

_____.

Definitions

For the avoidance of doubt, and for consistency in terminology, the following definitions will apply within this Policy.

Data	This includes both automated and manual data. Automated data means data held on computer, or stored with the intention that it is processed on computer. Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.
Personal Data	Information which relates to a living individual, who can be identified either directly from that data, or indirectly in conjunction with other data which is likely to come into the legitimate possession of the Data Controller. (If in doubt, [The Company] refers to the definition issued by the Article 29 Working Party, and updated from time to time.)
Sensitive Personal Data	A particular category of Personal data, relating to: Racial or Ethnic Origin, Political Opinions, Religious, Ideological or Philosophical beliefs, Trade Union membership, Information relating to mental or physical health, information in relation to one's Sexual Orientation, information in relation to commission of a crime and information relating to conviction for a criminal offence.
Data Controller	A person or entity who, either alone or with others, controls the content and use of Personal Data by determining the purposes and means by which that Personal Data is processed.
Data Subject/Member/ registrant	A living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.
Data Processor	A person or entity who processes Personal Data on behalf of a Data Controller on the basis of a formal, written contract, but who is not an employee of the Data Controller, processing such Data in the course of his/her employment.
Data Protection Officer	A person appointed by [The Company] to monitor compliance with the appropriate Data Protection legislation, to deal with Subject Access Requests, and to respond to Data Protection queries from staff members and service recipients
Relevant Filing System	Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers), and that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.

HETI's Data Loss Notification Procedure

Introduction:

The purpose of this document is to provide a concise procedure to be followed in the event that HETI becomes aware of a loss of personal data. This includes obligations under law, namely the Irish Data Protection Act (1988), and the Irish Data Protection (Amendment) Act (2003).

The procedure is consistent with the guidelines issued by the Irish Data Protection Commissioner in 2010, and enshrined in Irish law.

Rationale:

The response to any breach of personal data (as defined by the legislation) can have a serious impact on HETI's reputation and the extent to which the public perceives HETI as trustworthy.

The consequential impact on the organisation can be immeasurable. Therefore, exceptional care must be taken when responding to data breach incidents. Not all data protection incidents result in data breaches, and not all data breaches require notification. This guide is to assist staff/Board members/volunteers in developing an appropriate response to a data breach based on the specific characteristics of the incident.

Scope:

The policy covers both personal and sensitive personal data held by HETI. The policy applies equally to personal data held in manual and automated form.

All Personal and Sensitive Personal Data will be treated with equal care by HETI. Both categories will be equally referred-to as Personal Data in this policy, unless specifically stated otherwise.

This policy should be read in conjunction with the associated Data Protection Policy, Subject Access Request procedure, the Data Retention and Destruction Policy and the Data Retention Periods List.

What constitutes a breach, potential or actual?

A breach is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, for an authorized purpose, have access or potential access to personal data in usable form, whether manual or automated.

This could mean:

- Loss of a laptop, memory stick or mobile device that contains personal data
- Lack of a secure password on pc's and applications
- Emailing a list of students to someone in error
- Giving a system login to an unauthorised person
- Failure of a door lock or some other weakness in physical security which compromises personal data

What happens if a breach occurs?

Actual, suspected, or potential breaches should be reported immediately to HETI's Data Protection Officer (DPO) or IT Administrator (ITA).

A team comprising the DPO, ITA and other relevant staff /board members will be established to assess the breach and determine its severity. Depending on the scale and sensitivity of data lost and the number of Data Subjects impacted, the Office of the Data Protection Commissioner and relevant regulatory bodies will be informed as quickly as possible following detection.

In certain circumstances HETI may (e.g. if required by the Office of the Data Protection Commissioner), inform the data subjects of the loss of their data and provide them with an assessment of the risk to their privacy. HETI will make recommendations to the data subjects which may minimise the risks to them. HETI will then implement changes to procedures, technologies or applications to prevent a recurrence of the breach.

When will the Office of the Data Protection Commissioner be informed?

All incidents in which personal data has been put at risk will be reported to the Office of the Data Protection Commissioner. The only exceptions to this policy are when the data subjects have already been informed, where the loss affects fewer than 100 data subjects, and where the loss involves only non-sensitive, non-financial personal data.

Where devices or equipment containing personal or sensitive personal data are lost or stolen, the Data Protection Commissioner is notified only where the data on such devices is not encrypted.

Data Loss Incident logging.

All data breaches will be recorded in an incident log as required by the Office of the Data Protection Commissioner. The log will maintain a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record will include a brief description of the nature of the incident and an explanation of why the Office of the Data Protection Commissioner was not informed. Such records will be provided to the Office of the Data Protection Commissioner upon request.

Related Policies and Procedures:

- Record Retention and Destruction Policy
- Data Loss Incident Log

This Policy was approved by the Board of Directors of HETI on _____.

HETI's Record Retention Policy

Purpose

The purpose of this Policy is to ensure that necessary records and documents of HETI are adequately protected and maintained and to ensure that records that are no longer needed by HETI or are of no value are discarded at the proper time. This Policy is also for the purpose of aiding employees and board members of HETI in understanding their obligations in retaining electronic documents - including e-mail, Web files, text files, sound and movie files, PDF documents, and all Microsoft Office or other formatted files.

1) Policy

This Policy represent's HETI's policy regarding the retention and disposal of records and the retention and disposal of electronic documents.

2) Administration

Attached as Appendix A is a Record Retention Schedule that is approved as the initial maintenance, retention and disposal schedule for physical records of HETI and the retention and disposal of electronic documents. The Executive Director/Secretary is the officer in charge of the administration of this Policy and the implementation of processes and procedures to ensure that the Record Retention Schedule is followed. The Executive Director/Secretary is also authorized to: make modifications to the Record Retention Schedule from time to time to ensure that it is in compliance with local, state and federal laws and includes the appropriate document and record categories for HETI; monitor local, state and federal laws affecting record retention; annually review the record retention and disposal program; and monitor compliance with this Policy.

This Policy applies to all physical records generated in the course of HETI's operation, including both original documents and reproductions. It also applies to the electronic documents described above.

This Policy was approved by the Board of Directors of HETI on _____.

APPENDIX A - RECORD RETENTION SCHEDULE

The Record Retention Schedule is organized as follows:

SECTION TOPIC

A. Accounting and Finance
B. Contracts
C. Corporate Records
D. Correspondence and Internal Memoranda
E. Electronic Documents
F. Grant Records
G. Insurance Records
H. Legal Files and Papers
I. Miscellaneous

A. ACCOUNTING AND FINANCE

Record Type	Retention Period
Accounts Payable ledgers and schedules	7 years
Accounts Receivable ledgers and schedules	7 years
Tri -Annual Audit Reports and Financial Statements	Permanent
Tri-Annual Audit Records, including work papers and other documents that relate to the audit	7 years after completion of audit
Annual Plans and Budgets	7 Years
Bank Statements and Canceled Cheques	7 years
Employee Expense Reports	7 years
General Ledgers	Permanent
Interim Financial Statements	7 years
Notes Receivable ledgers and schedules	7 years
Investment Records	7 years after sale of investment
Credit card records (documents showing customer credit card number)	13 months

1. Credit card record retention and destruction

A credit card may be used to pay for the following HETI products and services: Membership, publications, donations and sponsorship .

All records showing customer credit card number must be locked in a desk drawer or a file cabinet when not in immediate use by staff/board members.

If it is determined that information on a document, which contains credit card information, is necessary for retention beyond 2 years, then the credit card number will be cut out of the document.

B. CONTRACTS

Record Type	Retention Period
Contracts and Related Correspondence (including any proposal that resulted in the contract and all other supportive documentation)	7 years after expiration or termination

C. ORGANISATION RECORDS

Record Type	Retention Period
Organisation Records (minute books, signed minutes of the Board and all committees, corporate seals, articles of association, bylaws, annual corporate reports)	Permanent
Licenses and Permits	Permanent

D. CORRESPONDENCE AND INTERNAL MEMORANDA

General Principle: Most correspondence and internal memoranda should be retained for the same period as the document they pertain to or support. For instance, a letter pertaining to a particular contract would be retained as long as the contract (7 years after expiration). It is recommended that records that support a particular project be kept with the project and take on the retention time of that particular project file.

Correspondence or memoranda that do not pertain to documents having a prescribed retention period should generally be discarded sooner. These may be divided into two general categories:

1. Those pertaining to routine matters and having no significant, lasting consequences should be discarded *within two years.* Some examples include:

    - Routine letters and notes that require no acknowledgment or follow-up, such as notes of appreciation, congratulations, letters of transmittal, and plans for meetings.
    - Form letters that require no follow-up.
    - Letters of general inquiry and replies that complete a cycle of correspondence.
    - Letters or complaints requesting specific action that have no further value after changes are made or action taken (such as name or address change).
    - Other letters of inconsequential subject matter or that definitely close correspondence to which no further reference will be necessary.
    - Chronological correspondence files.

    Please note that copies of interoffice correspondence and documents where a copy will be in the originating department file should be read and destroyed, unless that information provides reference to or direction to other documents and must be kept for project traceability.

2. Those pertaining to non-routine matters or having significant lasting consequences should generally be retained permanently.

E. ELECTRONIC DOCUMENTS

1. **Electronic Mail**: Not all email needs to be retained, depending on the subject matter.
    - All e-mail—from internal or external sources—is to be deleted after 12 months.
    - Staff will strive to keep all but an insignificant minority of their e-mail related to business issues.
    - HETI will archive e-mail for 12 months after the staff has deleted it, after which time the e-mail will be permanently deleted.
    - All HETI business-related email should be downloaded to a service center or user directory on the server.
    - Staff will not store or transfer HETI -related e-mail on non-work-related computers except as necessary or appropriate for HETI purposes.
    - Staff will take care not to send confidential/proprietary HETI information to outside sources.

F. GRANT RECORDS

Record Type	Retention Period
Original grant proposal	7 years after completion of grant period
Grant agreement and subsequent modifications, if applicable	7 years after completion of grant period
All requested IRS/grantee correspondence including determination letters and “no change” in exempt status letters	7 years after completion of grant period
Final grantee reports, both financial and narrative	7 years after completion of grant period
All evidence of returned grant funds	7 years after completion of grant period
All pertinent formal correspondence including opinion letters of counsel	7 years after completion of grant period
Report assessment forms	7 years after completion of grant period
Documentation relating to grantee evidence of invoices and matching or challenge grants that would support grantee compliance with the grant agreement	7 years after completion of grant period
Pre-grant inquiry forms and other documentation for expenditure responsibility grants	7 years after completion of grant period
Grantee work product produced with the grant funds	7 years after completion of grant period

Record Type	Retention Period
Legal Memoranda and Opinions (including all subject matter files)	7 years after close of matter
Litigation Files	1 year after expiration of appeals or time f filing appeals
Court Orders	Permanent
Requests for Departure from Records Retention Plan	10 years

Record Type	Retention Period

7	Years

Consultant's Reports	
Material of Historical Value (including pictures, publications)	Permanent
Policy and Procedures Manuals – Original	Current version with revision history
Policy and Procedures Manuals - Copies	Retain current version only
Annual Reports	Permanent

Record Type	**Retention Period**
Employee Deduction Authorizations	4 years after termination
Payroll Deductions	Termination + 7 years
W-2 and W-4 Forms	Termination + 7 years
Garnishments, Assignments, Attachments	Termination + 7 years
Labor Distribution Cost Records	7 years
Payroll Registers (gross and net)	7 years
Time Cards/Sheets	2 years
Unclaimed Wage Records	6 years

General Principle: Donors Forum must keep books of account or records as are sufficient to establish amount of gross income, deductions, credits, or other matters required to be shown in any such return.

These documents and records shall be kept for as long as the contents thereof may become material in the administration of federal, state, and local income, franchise, and property tax laws.

Record Type	**Retention Period**
Tax-Exemption Documents and Related Correspondence	Permanent
IRS Rulings	Permanent
Excise Tax Records	7 years

Record Type	Retention Period
Payroll Tax Records	7 years
Tax Bills, Receipts, Statements	7 years
Tax Returns - Income, Franchise, Property	Permanent
Tax Workpaper Packages - Originals	7 years
Sales/Use Tax Records	7 years
Annual Information Returns - Federal and State	Permanent
IRS or other Government Audit Records	Permanent

Record Type	Retention Period
Records of Contributions	Permanent
HETI's or other documents evidencing terms of gifts	Permanent
Research & Publications	Permanent (1 copy only)

Record Type	Retention Period
Sponsorship agreements	Permanent