Data Protection Policy

Title:	Data Protection Policy
Reference/version no:	2
Status:	Approved
Approval date:	April 2022
Next review date	June 2024
Background:	Outward facing policy - posted online

Contents

1. About Mental Health Reform 3
2. Data Protection 3
3. The GDPR 3
4. Other Terms Used in this Policy 3
5. Policy statement 4
6. How People Provide MHR with Personal Information 4
7. Why MHR Collects Information 5
8. How MHR Uses the Information Collected 5
9. Disclosure of Personal Information 6
10. Retaining Personal Information 6
11. Subject Access Requests and Data Subjects Rights 6
12. Security of Personal Data 7
13. Data Retention Policy and Schedule 7
14. Grounds for Processing Personal Data 7
15. Document Retention Procedure 8
16. Data Breach Notification 8
17. Records 8
18. Disposable Information 9
19. Confidential Information Belonging to Others 9
20. Role of Operations and Office Coordinator 10
21. Storage and Destruction of Records 10
22. Questions About the Policy 11
23. Changes to this Policy 11
24. MHR Record Retention Schedule 12

1. About Mental Health Reform

Mental Health Reform (MHR) is the national coalition of organisations campaigning to transform mental health and wellbeing supports in Ireland. MHR was formed in 2006 and has over 70 member organisations representing a range of interests. The registered offices of MHR are Coleraine House, Coleraine Street, Dublin 7.
This document provides information about the ways in which MHR processes, stores and secures personal data.

2. Data Protection

Data Protection is the means by which the privacy rights of individuals are safeguarded in relation to the processing of their personal data. The Data Protection Acts 1988 and 2003 confer rights on individuals as well as placing responsibilities on those persons processing personal data.

3. The GDPR

The General Data Protection Regulation (GDPR) is in force as of the 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive. The GDPR relies on seven principles, which will regulate the processing of personal data. These principles are:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

General information on the GDPR is available from the website of the Data Protection Commission https://www.dataprotection.ie/

4. Other Terms Used in this Policy

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.

Processing means 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.

Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future.

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

Data controller means 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 processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Third party means 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.

Personal data breach means 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.

Supervisory Authority means an independent public authority which is established by a Member State pursuant to Article 51.

5. Policy statement

MHR will process any personal information provided to it by individuals, whether it be provided through our website, in person, by any form, correspondence, telephone, email or by any other means, or otherwise held by us in relation to data subjects in the manner set out in this policy.

6. How People Provide MHR with Personal Information

People may provide MHR with information by:

- Contacting us by letter, telephone, e-mail or in person;

- Subscribing to the MHR newsletter or E-zine (electronic magazine);
- Registering for a MHR event;
- Applying for membership of MHR;
- Donating to MHR;
- Applying to work with MHR as an employee or volunteer.
- Visiting the MHR website.[1]

Mental Health Reform will only ever ask data subjects to disclose only as much information as is necessary for the purpose of their interaction with us or when submitting a question/suggestion/comment in relation to our website or our services.

7. Why MHR Collects Information

MHR collects information in order to function effectively as an organisation, to communicate with our membership, to campaign, to fundraise, to improve our website, to recruit staff and volunteers, to host events and undertake research or other related activities.

8. How MHR Uses the Information Collected

MHR will use the information collected to:

- process enquiries;
- liaise with individuals about projects that MHR are involved in;
- comply with obligations arising from contracts entered into;
- register people for MHR events;
- provide people with news about MHR;
- process a membership enquiry, application or payment;
- set up, operate and manage a fundraising event or initiative;
- comply with our legal duties and responsibilities;
- provide security to, and ensuring the health and safety of, employees, volunteers and visitors to company premises;
- administer and improve MHR website and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes;
- as part of MHR efforts to keep its website safe and secure

[1] This type of data may include traffic data, location data, weblogs and other communication data that may identify personal information (e.g. cookies) and non-personal information (e.g. information of an anonymised or technical nature). See our cookie policy for more information.

MHR does not engage in any automated decision making processes nor do we use any personal data as a basis for any such automated decisions.

9. Disclosure of Personal Information

MHR may share personal data with selected third parties including, business partners, suppliers and sub-contractors for the performance of any contract we enter into with them or with data subjects and to assist us in fulfilling our functions such as:

- Cloud Service Providers;
- CRM providers;
- Archive/shredding companies;
- Email and ICT service providers.

10. Retaining Personal Information

The time periods for which we retain personal data depends on the type of information and the purposes for which we use it. We will keep your information for no longer than is required or permitted. MHR does not transfer data outside of the EU.

11. Subject Access Requests and Data Subjects Rights

The GDPR and Data Protection Acts give individuals the right to access information held about them by MHR. MHR must respond to all requests for personal information and will normally provide information free of charge. Individuals may request to see any personal information MHR holds about them including copies of email correspondence.

MHR will manage requests in a timely manner within the timelines stipulated by the GDPR and Data Protection Act 2018.

Where a data subject makes a formal request to MHR with respect to the information held by MHR, such a request gives rise to the following access rights under the GDPR and in accordance with the Data Protection Act 2018:

- The right to be informed, i.e. the right to access the information MHR holds about them
- The right of access
- The right to erasure, i.e. the right to have MHR erase any information we hold about them in circumstances such as where it is no longer necessary for us to hold the information for or if data subjects withdraw consent to the processing;
- The right of rectification, i.e. the right to require MHR to rectify any inaccurate information about them without undue delay
- The right to restrict processing
- The right to object, i.e. the right to object to MHR processing information about them

- The right to data portability, i.e. the right to ask MHR to provide their personal data in a portable format or, where technically feasible, for MHR to port that information to another provider, provided it does not result in a disclosure of information relating to other people
- The right to withdraw consent for data processing
- Rights with respect to data profiling and automated decision-making

When MHR processing of personal data is based on consent, the data subject has the right to withdraw that consent at any time, but any processing that MHR has carried out before consent is withdrawn remains lawful.

12. Security of Personal Data

MHR will take all reasonable steps to secure personal data from unauthorised access, use or disclosure.

13. Data Retention Policy and Schedule

The Data Protection Acts 1988 and 2003 (as amended) and the General Data Protection Regulation (GDPR) impose obligations on MHR, as a Data Controller, to process personal data in a fair manner which notifies data subjects of the purposes of data processing and to retain the data for no longer than is necessary to achieve those purposes.

Data subjects have a right to be informed about how their personal data is processed. The GDPR sets out the information that MHR should supply to individuals and when individuals should be informed of this information. MHR is obliged to provide data subjects with information on retention periods and criteria used to determine the retention periods.

14. Grounds for Processing Personal Data

MHR is required to provide data subjects with the legal grounds or lawful basis that they are relying on for processing personal data.
The legal grounds for processing personal data are as follows:

- Consent;
- Performance of a contract;
- Legal obligation;
- Vital interest;
- Public interest;

Explicit consent or an alternative limited lawful basis is required where sensitive personal data is being processed.

If there is no justification for retaining personal information, then that information should be routinely deleted. Information should never be kept "just in case" a use can be found for it in the future.

15. Document Retention Procedure

MHR is required to retain certain records, usually for a specific amount of time. The accidental or intentional destruction of these records during their specified retention periods could result in the following consequences:

- Fines and penalties;
- Loss of rights;
- Obstruction of justice charges;
- Contempt of court charges;
- Serious disadvantages in litigation;
- Disadvantage to the owner of the data

MHR must retain certain records because they contain information that:

- Serves as MHR's organisational memory;
- Have enduring business value (for example, they provide a record of a business transaction, evidence MHR's rights or obligations, protect our legal interests or ensure operational continuity;
- Must be kept in order to satisfy legal, accounting or other regulatory requirements.

16. Data Breach Notification

MHR treat data breaches very seriously. Any staff member or volunteer who becomes aware of a likely data breach and fails to notify the Data Protection Liaison Contact, may be subject to the MHR's disciplinary procedures depending on the severity of the breach.

17. Records

A record is any type of information created, received or transmitted in the transaction of MHR's business, regardless of physical format. Examples of where the various types of information are located are:

- Appointment books and calendars;
- Audio and video recordings;
- Computer programs;
- Contracts;
- Electronic files;

- E-mails;
- Handwritten notes;
- Invoices;
- Letters and other correspondence;
- Memory in mobile phones and portable devices;
- Online postings, such as on Facebook, Twitter, Instagram, LinkedIn and other sites;
- Membership applications;
- Performance reviews;
- Photographs;
- Voicemails.

Therefore, any paper records and electronic files that are part of any of the categories listed in the Retention Schedule contained in this policy, must be retained for the amount of time indicated in the Retention Schedule.

A record must not be retained beyond the period indicated in the Retention Schedule, unless a valid business reason (or a litigation hold or other special situation) calls for its continued retention.

18. Disposable Information

Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a record as defined by this policy. Examples may include:

- Duplicates of originals that have not been annotated;
- Preliminary drafts of letters, memoranda, reports, worksheets and informal notes that do not represent significant steps or decisions in the preparation of an official record;
- Books, periodicals, manuals, training binders and other printed materials obtained from sources outside of MHR and retained primarily for reference purposes; and
- Spam and junk mail.

19. Confidential Information Belonging to Others

Any confidential information that an employee may have obtained from a source outside of MHR, such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by MHR. Unsolicited confidential information submitted to MHR should be refused, returned to the sender where possible and deleted, if received via the internet.

20. Role of Operations and Office Coordinator

The Operations and Office Coordinator, in conjunction with the CEO, is responsible for identifying the documents that MHR must or should retain.
The responsibilities of the Operations and Office Coordinator include:

- Arranging for the proper storage and retrieval of records, coordinating with outside vendors where appropriate
- Handling the destruction of records whose retention period has expired without further notice that the records are being destroyed
- Planning, developing and prescribing document disposal policies, systems, standards and procedures
- Monitoring compliance so that employees know how to follow the document management procedures
- Developing and implementing measures to ensure that the CEO knows what information MHR has and where it is stored, that only authorised users have access to the information, and that MHR keeps only the information it needs, thereby efficiently using space
- Establishing standards for filing and storage equipment and recordkeeping supplies
- Identifying essential records and establishing a disaster plan for each office and department to ensure maximum availability of MHR's records in order to re-establish operations quickly and with minimal interruption and expense
- Determining the practicability of and, if appropriate, establishing a uniform filing system and a forms design and control system
- Periodically reviewing the records retention schedules and legislation to determine if MHR's document management program and its Records Retention Schedule is in compliance with legislation
- Explaining to employees their duties relating to the document management program
- Ensuring that the maintenance, preservation, microfilming, computer disk storage, destruction or other disposition of MHR'S records is carried out in accordance with this policy, the procedures of the document management program and our legal requirements
- Planning the timetable for an annual records destruction exercise and records audit
- Evaluating the overall effectiveness of the document management program

21. Storage and Destruction of Records

MHR's records must be stored in a safe, secure and accessible manner.

The Operations and Office Coordinator is responsible for the continuing process of identifying the records that have met their required retention period and supervising their destruction. The destruction of personal data, confidential, financial and personnel-related paper records must be conducted by confidential shredding.

22. Questions About the Policy

Any questions about this policy should be referred to the Operations and Office Coordinator who is in charge of administering and updating this policy.

The contact details for MHR's designated Data Protection Liaison is:

Name: Wendy Mitchell

Company Postal Address: Coleraine House, Coleraine Street, Dublin 7

Telephone: 01 8749468

Email: info@mentalhealthreform.ie

23. Changes to this Policy

Any changes to this Data Protection Policy and Data Retention Schedule will be approved by the Board of Directors and published on the website of Mental Health Reform.

24. MHR Record Retention Schedule

Personnel Records

Record	Retention Period	Justification
Benefits descriptions per employee	Permanent	Irish employment law and for pension calculation and record keeping
Employee applications and resumes	1 year or where successful, for the duration of the employment plus 7 years from the date of termination of employment	Irish employment law and for record keeping
Employee benefit plans	6 years from when the record was required to be disclosed save pension detail requirements	Benefit of the employee
Employee offer letters (and other documentation regarding hiring, promotion, demotion, transfer, termination or selection for training)	6 years from date of making record or action involved, whichever is later, or 1 year from date of involuntary termination	Benefit of the employee
Records relating to background checks on employees	6 years from when the background check is conducted	Irish employment law
Employment contracts; employment and termination agreements	7 years from the date of expiry of the contract or agreement	Benefit of the employee
Employee records with information on pay rate or weekly compensation	3 years	Benefit of the employee
Tax forms	6 years after date of hire	Revenue obligation
Injury and Illness Incident Reports and related Annual Summaries; Logs of work-related injuries and illnesses	6 years following the end of the calendar year that these records cover	Statute of Limitations
Supplemental record for each occupational injury or illness; Log and Summary of Occupational Injuries and Illnesses	6 years following the year to which they relate	Statute of Limitations
Job descriptions, performance goals and reviews; garnishment records	For the duration of the employment plus 7 years from the date of termination of employment	Benefit of employee
Employee tax records	6 years from the date tax is due or paid	Revenue obligations
Medical exams required by law	Duration of employment + 30 years	Benefit of employee

Personnel or employment records	6 years from the date the record was made	Benefit of employee
Pension plan and retirement records	Permanent	Benefit of employee
Pre-employment tests and test results	2 years from date of termination	Benefit of employee
Salary schedules; ranges for each job description	2 years	Benefit of employee
Time reports	Termination + 3 years	Benefit of employee
Training agreements, summaries of applicants' qualifications, job criteria, interview records	Duration of training + 4 years	Benefit of employee

Payroll Records

Record	Retention Period	Justification
Payroll registers (gross and net)	3 years from the last date of entry	Benefit of employee
Time cards; piece work tickets; wage rate tables; pay rates; work and time schedules; earnings records; records of additions to or deductions from wages; records on which wage computations are based	7 years	Benefit of employee

Prospective employees/volunteers

Record	Retention Period	Justification
Curriculum vitae and cover letters	12 months	For future employment opportunities
Interview notes	12 months	For future employment opportunities

Tax Records

Record	Retention Period	Justification
All tax records	7 years	Revenue Requirements

Accounting and Finance

Record	Retention Period	Justification
Accounts Payable, Receivables ledgers and schedules	7 years	Revenue Requirements
Annual audit reports and financial statements	Permanent	Revenue Requirements
Annual plans and budgets	2 years	Revenue Requirements
Bank statements, cancelled checks, deposit slips	7 years	Revenue Requirements
Business expense records	7 years	Revenue Requirements
Cash receipts	2 years	Revenue Requirements
Details of cheques	7 years	Revenue Requirements
Electronic fund transfer documents	7 years	Revenue Requirements
Employee expense reports	7 years	Revenue Requirements
General ledgers	Permanent	Revenue Requirements
Journal entries	7 years	Revenue Requirements
Invoices	7 years	Revenue Requirements
Petty cash vouchers	3 years	Revenue Requirements

Legal and Insurance Records

Record	Retention Period	Justification for time frame
Appraisals	6 years from termination	
Insurance claims/ applications	Permanent	Revenue Requirements
Insurance disbursements and denials	Permanent	
Insurance contracts and policies (Director and Officers, General Liability, Property, Workers' Compensation)	Permanent	
Leases	6 years after expiration	
Real estate documents (including loan and mortgage contract, deeds)	Permanent	
Warranties	Duration of warranty + 7 years	