


Policy

Title: GDPR Policy

Document No.	Version	Status	Effective Date
POL-05	02	Approved	29/05/2020

Document Approvals

	Print Name	Signature	Date
Approver	Fran Crowell		26/05/2020

1.0 Objective

This policy describes how Remember Us meets its obligations to individuals and the law regarding the safeguarding of personal data.

2.0 Scope

The scope of the document applies to all Staff of Remember Us.

3.0 Responsibilities

It is the responsibility of Remember Us to have a policy in place to meets its obligations to individuals and the law regarding the safeguarding of personal data.

4.0 Policy

The General Data Protection Regulation (GDPR) is in force as of the 25th of May 2018, replacing the existing data protection framework under the EU Data Protection Directive.

Introduction

Remember Us takes the safeguarding of personal information very seriously. In addition to the measures outlined in this policy, Remember Us takes particular care when handling the sensitive personal information entrusted to us by people who use our services.

These measures can be found in accompanying policies:

- Members records
- Managing Confidential Client Information

4.1 Fair Obtaining

Our data collection aims to be open and transparent at all times. At the time we collect information about individuals, they are made aware of how that information will be used.

Policy			
Title: GDPR Policy			
Document No.	Version	Status	Effective Date
POL-05	02	Approved	29/05/2020

Examples include - for assessment of application for service, for planning service delivery, for provision of information, research, recruitment and for marketing and fundraising purposes.

4.2 Purpose Specification

- i. Remember Us recognises the need to hold personal data about individuals for the following purposes:
 - Service provision and event coordination
 - Information communications
 - Fund-raising and development
 - Human Resources
- ii. At each point of data collection, we are clear to individuals about the purposes to which that information is being put.
- iii. Remember Us signup information allows people to specify the purpose of their consent, e.g., to receive Newsletters, e-Newsletters, info on events and SMS Text Messages.

4.2.1 Data Set Maintenance

The **General Manager** is the Data Protection Officer and has operational responsibility for maintaining the registration with the Data Protection Commissioner and the maintenance of all data sets associated with each purpose.

4.3 Use and Disclosure

- i. All Remember Us workers and volunteers are made aware of our policies through the induction process.
- ii. All Remember Us workers and volunteers are Garda Vetted and sign
 1. Media/Photographs consent form.
 2. Required standards of behaviour form
 3. Confidentiality Agreement.

Copies of all forms are retained in paper format currently and additionally maybe stored electronically in the future.

4.3.1 Disclosees

- i. There are special circumstances under which disclosure of personal data to third parties is allowed. These are provided for under the Data Protection legislation and are:
 - a. As ordered by the Gardai
 - b. For the purpose of investigating an offence
 - c. To prevent urgent injury or damage to person or property
 - d. Under a court order or other rule of law
 - e. Required for the purposes of obtaining legal advice or for legal proceedings in which the person making the disclosure is a party or a witness.
 - f. Made at the request of and with the consent of the subject of the data.

Policy			
Title: GDPR Policy			
Document No.	Version	Status	Effective Date
POL-05	02	Approved	29/05/2020

In all such cases, full reference will be made to the current legislation.

- ii. In these additional circumstances personal information may be released without the consent of persons served under the following conditions:
 - a. For use by any Remember Us employee who has a need for the information in the performance of their duties to ensure continuity of care.
 - b. To medical personnel who have a need for the information for the purpose of treating a condition which poses an immediate threat to the health of a person served (e.g. in the case of a seizure, or sudden collapse)
 - c. To government agencies or entities charged under applicable laws with the protection of public health and safety. In such cases, the information may be released with the consent of the individual whose records are being requested, or upon receipt of a written request from the relevant and appropriate representative of the government entity.
 - d. To relevant government agencies in relation to concerns regarding the health and wellbeing of minors.
 - e. To relevant health care professionals and/or designated next of kin if the person served presents with a significant risk to their own health or wellbeing (e.g., suicide risk).
 - f. To relevant government agencies and/or health care professionals (e.g., An Garda Síochána, Psychiatric services), in situations where the person served is deemed to pose a credible threat to the health/wellbeing of another person (e.g. staff member, another person served, member of the public)

4.4 Security

- i. Personal data is held within a number of secure systems within Remember Us, according to application. Personal data for client service provision is held in hard copy client files. Data for other applications is held on the internal network.
- ii. All personal data is maintained in a secure manner. The following physical and software safeguards are in place to protect personal data:

4.4.1 Confidential Client Records

- i. Information about clients kept in hard copy files under lock and key.
Responsibility: General Manager.

4.4.2 Human Resource Management System

- i. Human Resource paper files are maintained securely in locked cabinets with access controlled and limited to Human Resources Personnel and the General Manager.
- ii. Electronic records are maintained securely on a network drive with secure password.

Policy			
Title: GDPR Policy			
Document No.	Version	Status	Effective Date
POL-05	02	Approved	29/05/2020

Person Responsible: General Manager

4.4.3 Network Data

- i. All data held on Remember Us Networks is maintained on password protected PCs and is restricted access only to authorised employees.

Person responsible: General Manager

4.4.4 Laptop Security

- i. All Laptops for use with client personal data are Password Protected.
- ii. All data stored on hard drive(s) is encrypted.
- iii. Data stored on hard drives is protected by anti-virus software.

Person responsible – General Manager

4.5 Adequate, relevant and not excessive

- i. We collect and maintain sufficient information for the declared purpose in order to provide a fair and comprehensive service to each person.
- ii. We only hold that information which is adequate and relevant to the purpose it serves. If we are in receipt of personal data e.g in the form of medical records, which is extra to requirement, we ensure that the information is returned to the referring agent or destroyed as appropriate.
- iii. Reviews are conducted of the information collected on the referral form to ensure that it is sufficient and not excessive.
- iv. All records of staff client interactions are maintained in a professional manner are done so with the expectation that the information can be shared with the person served.

Person Responsible: General Manager.

4.6 Accurate and up to date

- i. Remember Us workers who maintain personal data are responsible for correcting and maintaining that information on an ongoing basis. For example:
 - a. Administration staff are responsible for maintaining the contact information and the personal data held by Remember Us,
 - b. The General Manager is responsible for maintaining the accuracy of fundraising lists.
 - c. The General Manager is responsible for maintaining the accuracy of distribution lists for newsletters.
 - d. The Human Resources Manager is responsible for maintaining the accuracy of the HR Management system.

4.7 Data Retention

- i. Personal information (e.g., about a member) processed/kept for any purpose should not be kept longer than is necessary for that purpose.
- ii. This gives some flexibility and Remember Us occasionally needs to make a professional judgement about how long is "necessary". The minimum period set down for the retention of records is eight years generally, 20 years in the

Policy

Title: GDPR Policy

Document No.	Version	Status	Effective Date
POL-05	02	Approved	29/05/2020

case of “mentally disordered persons”. Because litigation may occur some time after contact has finished, any destruction of material must be considered carefully if it is to be carried out before the minimum time period. Any such actions may need to be justified to others including the client.

Purpose	Retention Schedule
Information mailings	Data is retained for as long as mailing list is maintained, then subsequently deleted.
Fund-raising and development	Data is retained for as long as mailing list is maintained, then subsequently deleted.
Human Resources	See appendix 1 HR record retention schedule.

- iii. Purging of data occurs on an annual basis, and as once-offs on completion of purpose. All records will be destroyed in accordance with Data Protection law and Remember Us guidelines for retention and destruction as follows:
- iv. All records involved in any investigation, litigation, or audit will not be destroyed until legal counsel has confirmed that no further legal reason exists for retention of the record.
- v. In the event a legal proceeding is initiated against Remember Us, the General Manager will be notified immediately by a relevant Director to stop the destruction of files.
- vi. Prior to the destruction of records, the following information will be gathered from the record and permanently maintained for all persons served:
 - Person’s name.
 - PPS number if applicable
 - Date of birth.
 - Name and address of legal guardian, if any.
- vii. All records will be destroyed in a manner that eliminates the possibility of reconstruction of the information.
- viii. Paper records will be destroyed by shredding.
- ix. Any CD-RW disks that contain document imaging that cannot be overwritten will be destroyed through pulverisation.
- x. All activities related to the destruction of records will be documented and maintained by the General Manager. The following information will be included in the documentation of the destruction:
 - The date of the record destruction.
 - The method of destruction.
 - A description of the records that were destroyed.

Policy

Title: GDPR Policy

Document No.	Version	Status	Effective Date
POL-05	02	Approved	29/05/2020

- The start and end date of the records.
- The signatures of the individual conducting the destruction and of the witness of the action.

4.8 Your Rights with respect to personal data.

You have the following rights:

- to access the Personal Data and Special Categories of Personal Data your Company holds about you.
- to require your Company to rectify any inaccurate Personal Data or Special Categories of Personal Data about you without undue delay.
- to have your Company erase any Personal Data or Special Categories of Personal Data it holds about you in certain circumstances, for example where it is no longer necessary for your Company to hold the Personal Data or Special Categories of Personal Data for the purpose of your employment or if you have withdrawn your consent to the processing.
- to object to your Company processing your **Personal Data** or **Special Categories of Personal Data** in specific circumstances e.g., processing for profiling.
- to ask your Company to provide your **Personal Data** or **Special Categories of Personal Data** to you in a portable format or, where technically feasible, for it to port that information to another employer provided it does not result in a disclosure of information relating to other people.
- to request a restriction of the processing of your **Personal Data** or **Special Categories of Personal Data**.
- in the limited circumstances where you may have provided your consent to the collection, processing and transfer of your **Personal Data** or **Special Categories of Personal Data** for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. Once your Company has received notification that you have withdrawn your consent, your Company will no longer process your information for the purpose or purposes you originally agreed to, unless your Company has another legitimate basis for doing so in law. In that instance, any processing that your Company has carried out, before you withdrew your consent, remains lawful.
- A right not to be subject to automated decision making.
- The right to receive notification of a **Personal Data Breach**.
- Where processing is based on consent, the right to withdraw such consent.
- The right to lodge a complaint to the Data Protection Commission.

4.9 Registration

- Remember Us shall be registered with the Data Protection Commissioner. Registration is maintained by the General Manager and is reviewed and renewed as required.

Policy			
Title: GDPR Policy			
Document No.	Version	Status	Effective Date
POL-05	02	Approved	29/05/2020

4.10 Training & Education

- i. This policy is circulated to all new staff as part of their induction process.
- ii. Awareness of Data protection issues is through updates from the General Manager.

4.11 Co-ordination and Compliance

- ii. The data protection co-ordinator and compliance person is the General Manager.
 - i. All staff are made aware of this role via briefings.
 - ii. All breaches of this policy will be reported to the General Manager following the Data Loss Notification Procedure below.
 - iii. A formal review by the co-ordinator of data protection activities within Remember Us will take place periodically across the organisation.

5.0 Procedures

5.1 Personal Data Access Procedure

- All requests must be made in writing with the consent of the person served (excepting the conditions outlined under section 3. Vi and 3.vii in this policy).

- All requests should be made using the form attached (appendix 3) and sent to

General Manager
Remember Us
Unit 5
Balbriggan Retail Park
Balbriggan
Co. Dublin.
K32 K002

- Where requests are received in writing from 3rd parties, e.g., from solicitors or doctors, staff should check the validity of the request before notifying the General Manager. The request must quote the Data Protection legislation and also include the person served written consent.
- The General Manager must be notified of all requests for disclosure of personal information.
- The information will be supplied within one month of the request.

5.1.1 Requests made under the Freedom of Information Act (1997 and 2003)

- i. Remember Us is not a prescribed body under the terms of the Freedom of Information Act. However, records that are created in dedicated services subject to contracted service level agreements with HSE are deemed to be

Policy			
Title: GDPR Policy			
Document No.	Version	Status	Effective Date
POL-05	02	Approved	29/05/2020

held by the HSE and thus, may be subject to come within the scope of the act.

"Section 6(9) provides that the records of contractors to public bodies are deemed, insofar as they relate to the contracted service, to be held by the public body concerned."

- ii. Remember Us policy is to comply fully with all Freedom of Information requests made by the HSE under the terms of relevant service level agreements.
- iii. If a request is received by Remember Us under the terms of the Freedom of Information Acts, it should be immediately forwarded to the General Manager for further action and processing.

5.2 Procedure for Data Loss Notification

A breach is a loss of control, compromise, unauthorised disclosure, unauthorised acquisition, unauthorised access, or any similar term referring to situations where persons other than authorised users, for an authorised 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 confidential information to unauthorised person(s) 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

5.2.1 What happens if a breach occurs?

Actual, suspected, or potential breaches should be reported immediately to the General Manager.

5.2.2 Any employee who becomes aware of a likely data breach and fails to notify the General Manager will be subject to Remember Us disciplinary procedure.

A team comprising the General Manager and other relevant staff (which may include a Director) 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 Remember Us 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. Remember Us will make recommendations to the data subjects which may minimise the risks to them. Remember Us will then implement appropriate changes to procedures, technologies or applications to prevent a recurrence of the breach.

Policy

Title: GDPR Policy

Document No.	Version	Status	Effective Date
POL-05	02	Approved	29/05/2020

5.2.3 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.

5.2.4 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.

Policy

Title: GDPR Policy

Document No.	Version	Status	Effective Date
POL-05	02	Approved	29/05/2020

6.0 Appendices

Appendix 1 – Retention Schedule – HR records

General classes of records held HR	Default retention period	Final disposition
Annual/sick leave records	1 years	Destroy by confidential shredding
Time sheets	1 year	Destroy by confidential shredding
Records of staff training	5 years	Destroy by confidential shredding
Job description	Retain indefinitely	Archive
Applications and CV's of candidates who are called for interview	Retain for 2 years after closing of competition	Destroy by confidential shredding
Selection criteria	Retain indefinitely	Archive
Candidates not qualified or short listed	Retain list of candidates who applied, but destroy material such as application forms and CV's after 2 years.	Destroy by confidential shredding
Candidates short listed but not successful at interview or who are successful but do not accept offer	Retain for 1 year then destroy	Destroy by confidential shredding
Interview Board marking sheet and interview Board notes	Retain for 2 years then destroy	Destroy by confidential shredding
Finance/pension/retirement records	Retain until pensioner and dependent spouse are deceased and dependent children are finished full time education plus 3 years.	Destroy by confidential shredding
Staff Personnel Files	Retain for duration of employment. On retirement or resignation hold for a further six years but retain service records for finance/pension purposes. Destroy remainder listed below.	Destroy by confidential shredding
Application/CV	See above	
References	See above	
Recruitment medical	See above	
Contract/Job specification/Job description	See above	
Probation forms	See above	
Parental leave	Retain for 8 years	Destroy by confidential shredding

Policy

Title: GDPR Policy

Document No.	Version	Status	Effective Date
POL-05	02	Approved	29/05/2020

Discipline records	Hold on personal file/disciplinary file for duration of employment plus six years after resignation/retirement, then destroy. Where disciplinary policy provides for earlier removal destroy but keep a record that a warning was issued. Where the matter involved criminal activity, these records should be retained indefinitely.	Destroy by confidential shredding
Allegations and complaints	Where the complaint is found to be untrue or unwarranted make a note on personal file index that a complaint was made, but there is no need to keep detailed documentation or refer back to previous cases if further separate allegations are made in the future.	
Occupational health records	Depending on the types of materials to which the staff member was exposed (e.g. carcinogens) the health screening reports may need to be retained for up to 40 years. Consult with your local Health & Safety Officer about retention periods for this class of record.	
Industrial relations files	Hold policy documents and the history of their evolution indefinitely.	Archive
Agreements-pay and others	Retain indefinitely	Archive
Leave policy	Retain indefinitely	Archive
Employment policy	Retain indefinitely	Archive
Surveys/reports	Retain indefinitely	Archive
Union correspondence	Retain indefinitely	Archive
Individual industrial relations issues	Retain indefinitely	Archive
Minutes of meetings	Retain indefinitely	Archive
Labour Court Recommendations	Retain indefinitely	Archive
Contracts for services	Retain for the duration of the contract plus six years	Destroy by confidential shredding
Examples of contracts for services that may be held by Personnel/HR departments include EAP contracts with service providers and contracts with healthcare professionals.		

Policy			
Title: GDPR Policy			
Document No.	Version	Status	Effective Date
POL-05	02	Approved	29/05/2020

Appendix 2 Guidelines on Retention of Client Records

Type of information	Schedule	Comments
Records of people deceased by suicide	Retained for ten years following date of death	Notification of death by suicide must be made to Information and Support Manager
Records of people subject to unfinished court action, where known.	Retained indefinitely	Notification of applicable cases be made to Information and Support Manager
Clinicians notes/ Aide Memoires	Destroyed on completion of the service.	Maintained at discretion of clinician, these will be made anonymous and kept separate from the electronic, primary or secondary file
Individual records of the persons accessing Remember Us services following needs assessment	Retained for eight years after the most recent discharge date.	Paper and electronic media
Individual records of the persons attending needs assessment but subsequently deemed ineligible for services or clients who have been invited to needs assessment but decline to attend	Retained for eight years following final closure of case.	Paper and electronic media
All preadmission application and screening records of persons deemed not eligible to Remember Us services at that time (i.e. not attending needs assessment)	Paper file maintained for five years , together with a note explaining the reason for non-admittance (e.g. “does not meet criteria”). Forms having no identifiable information regarding the person	

Policy

Title: GDPR Policy

Document No.	Version	Status	Effective Date
POL-05	02	Approved	29/05/2020

	served will be destroyed in one year .	
External referral forms for referrals to Remember Us	To be included in the record for persons admitted and will be retained for the same period as the record itself (see above)	
Information for statistical/ Audit purposes	There will be no time limit on such information being retained at this generally will be anonymous.	Information to be held anonymously where possible. Exceptions may need to be made for purposes of funder reports, accreditation audits.

Policy

Title: GDPR Policy

Document No.	Version	Status	Effective Date
POL-05	02	Approved	29/05/2020

Appendix 3 – Personal Data Request Form

Personal Data Request Form

Data Protection Officer
Remember Us
Unit 5
Balbriggan Retail Park.
Balbriggan
Co. Dublin
K32 K002

[Date]

Dear Sir/Madam,

I wish to make an access request under the General Data Protection Regulation (GDPR) 2018 for a copy of any information you keep about me, on computer or in manual form. I am making this request under section 15 of the General Data Protection Regulation.

Regards

(signed)

[your name]

NAME (please print) _____

ADDRESS: _____

Please Note:

1. Request in writing should be made and signed by the applicant in person.
2. Within the terms of the General Data Protection Regulation 2018, Remember Us will respond to your request for personal data within one month of the request.
3. Requests should be submitted to: Data Protection Office, Remember Us, Unit 5, Balbriggan Retail Park, Balbriggan, Co. Dublin, K32 K002.

Policy

Title: GDPR Policy

Document No.	Version	Status	Effective Date
POL-05	02	Approved	29/05/2020

6.0 Revisions

Version Number	Description of Revision
01	First issuance of Policy for GDPR
02	Review and update of format