

The Rehab Group Data Protection Policy


Applies Jurisdiction: ALL

Division: ALL

Reference Number: COR-DAM-001

Version Number: V3

Author(s): Margaret Murray
Title: Data Protection Officer
Date: March 2018

Approver(s): Pauline Newnham
Title: Director of Quality & Governance
Date: May 2018
Signature: 

Effective From: May 2018
Review Date: May 2021

| | | | | |
|-------------------------|--------------------|----------------------------------|--------------------------|--------------|
| Ref No.: COR-DAM-001 | Version No.: V3 | Policy Title: Data Protection | Review Date: May 2021 | Page 1 of 19 |
|-------------------------|--------------------|----------------------------------|--------------------------|--------------|

Rehab Group – Data Protection Policy

Table of Contents

1. Policy Statement
2. Purpose
3. Scope
4. Definitions
5. General Provisions /Procedure
6. Roles & Responsibilities
7. Evaluation and Audit
8. References
9. Appendices

| | | | | |
|-------------------------|--------------------|----------------------------------|--------------------------|--------------|
| Ref No.: COR-DAM-001 | Version No.: V3 | Policy Title: Data Protection | Review Date: May 2021 | Page 2 of 19 |
|-------------------------|--------------------|----------------------------------|--------------------------|--------------|

Rehab Group – Data Protection Policy

1.0 POLICY STATEMENT

This Policy sets out the obligations of The Rehab Group, regarding data protection and the rights of data subjects, in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation (“GDPR”) and as amended by national laws.

Ireland: The Data Protection Act(s) 1998, 2003 (as amended) and 2018 (when enacted)

United Kingdom: Data Protection Act 1998

Poland: Personal Data Protection Act 1997 “PDPA”

The GDPR defines “personal data” as any information relating to an identified or identifiable natural person (a “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.

This policy sets out The Rehab Group’s obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by The Rehab Group, its employees, agents, contractors, or other parties working on behalf of The Rehab Group.

The Rehab Group is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2.0 PURPOSE

This policy establishes an effective, accountable and transparent framework for ensuring compliance with the requirements of GDPR and national law. The GDPR sets out the following principles with which any party handling personal data must comply. All personal

| | | | | |
|-------------------------|--------------------|----------------------------------|--------------------------|--------------|
| Ref No.: COR-DAM-001 | Version No.: V3 | Policy Title: Data Protection | Review Date: May 2021 | Page 3 of 19 |
|-------------------------|--------------------|----------------------------------|--------------------------|--------------|

Rehab Group – Data Protection Policy

data must be;

- i. Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- ii. Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- iii. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- iv. Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.
- v. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.
- vi. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3.0 SCOPE

The policy covers both personal and sensitive personal data held in relation to data subjects by The Rehab Group. The policy applies equally to personal data held in manual and digital form.

All Personal and Sensitive Personal Data will be treated with equal care by The Rehab Group. Both categories will be equally referred to

| | | | | |
|-------------------------|--------------------|----------------------------------|--------------------------|--------------|
| Ref No.: COR-DAM-001 | Version No.: V3 | Policy Title: Data Protection | Review Date: May 2021 | Page 4 of 19 |
|-------------------------|--------------------|----------------------------------|--------------------------|--------------|

Rehab Group – Data Protection Policy

as Personal Data in this policy, unless specifically stated otherwise.

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

4.0 DEFINITIONS

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

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data.

Data Processor: the entity that processes data on behalf of the Data Controller.

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union.

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR.

Data subject: a natural person whose personal data is processed by a controller or processor.

Personal data: any information related to a natural person or 'data subject', which can be used to directly or indirectly identify the person.

| | | | | |
|-------------------------|--------------------|----------------------------------|--------------------------|--------------|
| Ref No.: COR-DAM-001 | Version No.: V3 | Policy Title: Data Protection | Review Date: May 2021 | Page 5 of 19 |
|-------------------------|--------------------|----------------------------------|--------------------------|--------------|

Rehab Group – Data Protection Policy

Data Protection Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data.

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour.

Regulation: a binding legislative act that must be applied in its entirety across the Union.

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them.

5.0 GENERAL PROVISIONS / PROCEDURE

The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

- The right to be informed (Part 5.1).
- The right of access (Part 5.2);
- The right to rectification (Part 5.3);
- The right to erasure (also known as the 'right to be forgotten') (Part 5.4);
- The right to restrict processing (Part 5.5);
- The right to data portability (Part 5.6);
- The right to object (Part 5.7); and
- Rights with respect to automated decision-making and profiling (Parts 5.8 and 5.9).

Lawful, Fair, and Transparent Data Processing

The GDPR seeks to ensure that personal data is processed lawfully,

| | | | | |
|-------------------------|--------------------|----------------------------------|--------------------------|--------------|
| Ref No.: COR-DAM-001 | Version No.: V3 | Policy Title: Data Protection | Review Date: May 2021 | Page 6 of 19 |
|-------------------------|--------------------|----------------------------------|--------------------------|--------------|

Rehab Group – Data Protection Policy

fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

- The data subject has given consent to the processing of their personal data for one or more specific purposes;
- The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
- The processing is necessary for compliance with a legal obligation to which the data controller is subject;
- The processing is necessary to protect the vital interests of the data subject or of another natural person;
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
- The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

If the personal data in question is “sensitive personal data” at least one of the following conditions must be met:

- The data subject has given their explicit consent to the processing of such data for one or more specified purposes;
- The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law;
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

Specified, Explicit, and Legitimate Purposes

The Rehab Group collects and processes personal data as set out in

| | | | | |
|-------------------------|--------------------|----------------------------------|--------------------------|--------------|
| Ref No.: COR-DAM-001 | Version No.: V3 | Policy Title: Data Protection | Review Date: May 2021 | Page 7 of 19 |
|-------------------------|--------------------|----------------------------------|--------------------------|--------------|

Rehab Group – Data Protection Policy

Part 5.1(a) of this Policy. This includes:

- Personal data collected directly from data subjects
- Personal data obtained from third parties by way of the referral pathway

The Rehab Group only collects, processes, and holds personal data for the specific purposes set out in Part 5.1(a) of this policy (or for other purposes expressly permitted by the GDPR and national law).

Data subjects are kept informed at all times of the purpose or purposes for which The Rehab Group uses their personal data.

Adequate, Relevant, and Limited Data Processing

The Rehab Group will only collect and process personal data for and to the extent necessary for the specific purpose of which data subjects have been informed (or will be informed) as under, and as set out in Part 5.1(a), below.

Accuracy of Data and Keeping Data Up-to-Date

The Rehab Group shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 5.3 below.

The accuracy of personal data shall be checked when it is collected. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

Data Retention

The Rehab Group shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

For full details of The Rehab Group's approach to data retention, including retention periods for specific personal data types held by The Rehab Group, please refer to our Data Retention & Destruction

| | | | | |
|-------------------------|--------------------|----------------------------------|--------------------------|--------------|
| Ref No.: COR-DAM-001 | Version No.: V3 | Policy Title: Data Protection | Review Date: May 2021 | Page 8 of 19 |
|-------------------------|--------------------|----------------------------------|--------------------------|--------------|

Rehab Group – Data Protection Policy

Policy.

Secure Processing

The Rehab Group shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

Data Protection Impact Assessments

The Rehab Group shall carry out Data Protection Impact Assessments (DPIA's) for any and all new projects and/or before the modification of existing technologies or processes; and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR.

Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

- The type(s) of personal data that will be collected, held, and processed;
- The purpose(s) for which personal data is to be used;
- The Rehab Group's objectives;
- The parties (internal and/or external) who are to be consulted;
- The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- Risks posed to data subjects;
- Risks posed both within and to The Rehab Group; and
- Proposed measures to minimise and address identified risks.

Data Breach Notification

All potential personal data breaches must be reported immediately to The Rehab Group's Data Protection Officer(s).

The Rehab Group's Data Protection Officers are:

Ireland & Poland Margaret Murray Margaret.murray@rehab.ie

| | | | | |
|-------------------------|--------------------|----------------------------------|--------------------------|--------------|
| Ref No.: COR-DAM-001 | Version No.: V3 | Policy Title: Data Protection | Review Date: May 2021 | Page 9 of 19 |
|-------------------------|--------------------|----------------------------------|--------------------------|--------------|

Rehab Group – Data Protection Policy

United Kingdom Mark Bibby MBibby@rehabgroup.eu

If a confirmed personal data breach occurs and that breach is likely to result in a confirmed risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Data Protection Authority is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Implementation of Policy

This policy shall be deemed effective as of **25 May 2018**. No part of this policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

5.1 Keeping Data Subjects Informed

The Organisation shall make available the information set out in part 5.1(a) to every data subject:

- Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
- Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
- if the personal data is used to communicate with the data subject, when the first communication is made; or
- if the personal data is to be transferred to another party, before that transfer is made; or
- as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

| | | | | |
|-------------------------|--------------------|----------------------------------|--------------------------|---------------|
| Ref No.: COR-DAM-001 | Version No.: V3 | Policy Title: Data Protection | Review Date: May 2021 | Page 10 of 19 |
|-------------------------|--------------------|----------------------------------|--------------------------|---------------|

Rehab Group – Data Protection Policy

5.1 (a) The following information shall be provided:

- Details of the organisation including, but not limited to, the identity of its Data Protection Officer;
- The purpose(s) for which the personal data is being collected and will be processed (as detailed in part 5.1(b) of this policy) and the legal basis justifying that collection and processing;
- Where applicable, the legitimate interests upon which the organisation is justifying its collection and processing of the personal data;
- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
- Where the personal data is to be transferred to one or more third parties, details of those parties;
- Details of data retention;
- Details of the data subject’s rights under the GDPR and the Data Protection Act 2018;
- Details of the data subject’s right to withdraw their consent to the organisation’s processing of their personal data at any time;
- Details of the data subject’s right to complain to the “supervisory authority” under the GDPR and the Data Protection Act 2018;
- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
- Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

5.1(b) Personal Data Collected, Held, and Processed

The following personal data is collected, held, and processed by The Rehab Group (for details of data retention and destruction, please refer to The Rehab Group’s Data Retention & Destruction Policy):

| | | | | |
|-------------------------|--------------------|----------------------------------|--------------------------|---------------|
| Ref No.: COR-DAM-001 | Version No.: V3 | Policy Title: Data Protection | Review Date: May 2021 | Page 11 of 19 |
|-------------------------|--------------------|----------------------------------|--------------------------|---------------|

Rehab Group – Data Protection Policy

| Data Ref. | Type of Data | Purpose of Data |
|--------------------------|--|---|
| Service User/ Student | Personal data - Name - Address - PPS number | Data is collected to allow Service Users / Students to avail of our services. |
| Service User/ Student | Sensitive Personal Data - Medical Report - Physiologist Report | Data is collected to allow Service Users / Students to be supported whilst they are in our services. |
| Staff Members | Personal Data - Name - Address - PPS Number | Recruitment Process. Employee Contract. Data is collected to allow staff members to be paid on a consistent and timely basis. |
| Staff Members | Sensitive Personal Data - Trade Union Membership -Physical or mental health data - Biometric Data | Data is collected to allow the Rehab Group to provide the best support for our staff members whilst in our organisation. |

5.2 Data Subject Access

- Data subjects may make data subject access requests (“DSARs”) at any time to find out more about the personal data which The Rehab Group holds about them, what it is doing with that personal data, and why.
- Employees wishing to make a DSAR should consult the Data Subject Access Request policy and send the request to the Rehab Group’s Data Protection Officer(s) at -
Ireland & Poland Margaret Murray, Roslyn Park, Beach Road,
Sandymount, Dublin 4

Rehab Group – Data Protection Policy

United Kingdom Margaret.murray@rehab.ie 01-2057219
Mark Bibby,
Mbibby@Rehabgroup.eu 0044 1 200 1140

- Responses to DSARs shall normally be made within 1 month of receipt, however this may be extended by a further two months if the DSAR is complex and/or numerous requests are made. The Controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.
- All DSARs received shall be managed by The Rehab Group's Data Protection Officer.
- The Rehab Group does not charge a fee for the handling of normal DSARs.

5.3 Rectification of Personal Data

Data subjects have the right to require The Rehab Group to rectify any of their personal data that is inaccurate or incomplete.

- The Rehab Group shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing The Rehab Group of the issue. The period can be extended by a further two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
- In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

5.4 Erasure of Personal Data

Data subjects have the right to request that The Rehab Group erases the personal data it holds about them in the following circumstances:

- It is no longer necessary for The Rehab Group to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
- The data subject wishes to withdraw their consent to The Rehab Group holding and processing their personal data; The data subject

| | | | | |
|-------------------------|--------------------|----------------------------------|--------------------------|---------------|
| Ref No.: COR-DAM-001 | Version No.: V3 | Policy Title: Data Protection | Review Date: May 2021 | Page 13 of 19 |
|-------------------------|--------------------|----------------------------------|--------------------------|---------------|

Rehab Group – Data Protection Policy

objects to The Rehab Group holding and processing their personal data (and there is no overriding legitimate interest to allow The Rehab Group to continue doing so) (see Part 5.7 of this policy for further details concerning the right to object);

- The personal data has been processed unlawfully;
- The personal data needs to be erased in order for The Rehab Group to comply with a particular legal obligation.

Unless The Rehab Group has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, without undue delay of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed; and

In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

5.5 Restriction of Personal Data Processing

Data subjects may request that The Rehab Group ceases processing the personal data it holds about them. If a data subject makes such a request, The Rehab Group shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

5.6 Data Portability

Where data subjects have given their consent to The Rehab Group to process their personal data, or the processing is otherwise required for the performance of a contract between The Rehab Group and the data subject, data subjects have the right, under the GDPR and the Data Protection Act 2018, to receive a copy of their personal data and

| | | | | |
|-------------------------|--------------------|----------------------------------|--------------------------|---------------|
| Ref No.: COR-DAM-001 | Version No.: V3 | Policy Title: Data Protection | Review Date: May 2021 | Page 14 of 19 |
|-------------------------|--------------------|----------------------------------|--------------------------|---------------|

Rehab Group – Data Protection Policy

to use it for other purposes (namely transmitting it to other data controllers).

To facilitate the right of data portability, The Rehab Group shall make available all applicable personal data to data subjects in the following formats:

- By email in pdf format
- By hard copy

Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by a further two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed within one month.

5.7 Objections to Personal Data Processing

Data subjects have the right to object to The Rehab Group processing their personal data based on legitimate interest.

- Where a data subject objects to The Rehab Group processing their personal data based on its legitimate interests, The Rehab Group shall cease such processing immediately, unless it can be demonstrated that The Rehab Group's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.
- Where a data subject objects to The Rehab Group processing their personal data for direct marketing purposes, The Rehab Group shall cease such processing immediately.

5.8 Profiling and Automated Decision Making

The Rehab Group will only engage in profiling and automated decision-making where it is necessary to enter into, or to perform, a contract with the data subject or where it is authorised by law. Where a service/entity utilises profiling and automated decision-making, this will be disclosed to the relevant data subjects. In such cases the data subject will be given the opportunity to:

| | | | | |
|-------------------------|--------------------|----------------------------------|--------------------------|---------------|
| Ref No.: COR-DAM-001 | Version No.: V3 | Policy Title: Data Protection | Review Date: May 2021 | Page 15 of 19 |
|-------------------------|--------------------|----------------------------------|--------------------------|---------------|

Rehab Group – Data Protection Policy

- Express their point of view
- Obtain an explanation for the automated decision
- Review the logic used by the automated system
- Supplement the automated system with additional data
- Have a human carry out a review of the automated decision
- Contest the automated decision
- Object to the automated decision-making being carried out

Each service/entity must also ensure that all profiling and automated decision-making relating to a data subject is based on accurate data.

5.9 Transferring Personal Data to a Country Outside the European Economic Area (EEA)

The Rehab Group may transfer personal data to internal or third party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. third countries), they must be made in compliance with an approved transfer mechanism. The Rehab Group may only transfer personal data where one of the transfer scenarios list below applies:

- The data subject has given consent to the proposed transfer;
- The transfer is necessary for the performance of a contract with the data subject;
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject's request;
- The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the data subject;
- The transfer is legally required on important public interest grounds;
- The transfer is necessary for the establishment, exercise or defence of legal claims;

| | | | | |
|-------------------------|--------------------|----------------------------------|--------------------------|---------------|
| Ref No.: COR-DAM-001 | Version No.: V3 | Policy Title: Data Protection | Review Date: May 2021 | Page 16 of 19 |
|-------------------------|--------------------|----------------------------------|--------------------------|---------------|

Rehab Group – Data Protection Policy

- The transfer is necessary in order to protect the vital interests of the data subject.

6.0 ROLES & RESPONSIBILITIES

The Rehab Group's Data Protection Officers are:

Ireland & Poland Margaret Murray
United Kingdom Mark Bibby

The Data Protection Officer shall be responsible for overseeing the implementation of this policy and for monitoring compliance with this policy, The Rehab Group's other data protection-related policies, and with the GDPR and other applicable data protection legislation.

The Rehab Group shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- The name and details of The Rehab Group, its Data Protection Officer, and any applicable third-party data processors;
- The purposes for which The Rehab Group collects, holds, and processes personal data;
- Details of the categories of personal data collected, held, and processed by The Rehab Group, and the categories of data subject to which that personal data relates;
- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
- Details of how long personal data will be retained by The Rehab Group (please refer to The Rehab Group's Data Retention & Destruction Policy); and
- Detailed descriptions of all technical and organisational measures taken by The Rehab Group to ensure the security of personal data.

7.0 EVALUATION & AUDIT

This policy will be reviewed every three years and in conjunction with legislative amendments, Rehab Group Guidelines and organisational requirements.

| | | | | |
|-------------------------|--------------------|----------------------------------|--------------------------|---------------|
| Ref No.: COR-DAM-001 | Version No.: V3 | Policy Title: Data Protection | Review Date: May 2021 | Page 17 of 19 |
|-------------------------|--------------------|----------------------------------|--------------------------|---------------|

Rehab Group – Data Protection Policy

8.0 REFERENCES

EU Regulation 2016/679 General Data Protection Regulation (“GDPR”)

National Laws

Ireland: The Data Protection Act(s) 1998, 2003 (as amended) and 2018 (when enacted)

United Kingdom: Data Protection Act 1998

Poland: Personal Data Protection Act 1997 “PDPA”

8.1 Related PPPGs

Data Retention & Destruction Policy

Data Breach Notification Policy

Data Subject Access Request Policy

9.0 APPENDICES

Appendix 1 – List of Authors

Appendix 2 – Read & Understood

| | | | | |
|-------------------------|--------------------|----------------------------------|--------------------------|---------------|
| Ref No.: COR-DAM-001 | Version No.: V3 | Policy Title: Data Protection | Review Date: May 2021 | Page 18 of 19 |
|-------------------------|--------------------|----------------------------------|--------------------------|---------------|

Rehab Group – Data Protection Policy

Appendix 1 – List of Authors

Authors List for New/ Reviewed Policy Area

The following names individual authors/ reviewers to this policy area.

| Division/Other | Name(s) |
|---|---------------------------------------|
| Regional Operating Officer | Cyril Gibbons |
| Regional Operating Officer | Rachael Thurlby |
| Regional Operating Officer | Grainne Fogarty |
| Regional Operating Officer | Jamie Lawson |
| Head of HR Business Partnering | Karen Fanneran |
| UK Business Support & Performance Manager | Caron Bozdugan |
| Barry Sweeney | Business Support & Performance Manger |
| Group Financial Controller | Ray Massey |
| Head of Public Affairs | Cathy Moore |
| Data Protection Officer | Mark Bibby |

*Note that it is not obligatory for each division to be involved in a new policy/ review if the policy is not relevant; this should be decided by each division on a case-by-case basis.

Appendix 2 – Read & Understood

I have read, understand and agree to adhere to the attached Data Protection Policy, Procedure, Protocol/ SOP or Guideline:

| Print Name | Signature | Date |
|------------|-----------|------|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

The Rehab Group Data Retention & Destruction Policy

Applies Jurisdiction: ALL
Division: ALL
Reference Number: COR-DAM-002
Version Number: V3

Author(s): Margaret Murray
Title: Data Protection Officer
Date: March 2018

Approver(s): Pauline Newnham
Title: Director of Quality & Governance
Date: May 2018
Signature: 

Effective From: May 2018
Review Date: May 2021

| | | | | |
|--------------------------------|---------------------------|---|---------------------------------|--------------|
| Ref No.: COR-DAM-002 | Version No.: V3 | Policy Title: Data Retention/ Destruction | Review Date: May 2021 | Page 1 of 30 |
|--------------------------------|---------------------------|---|---------------------------------|--------------|

Table of Contents

1. Policy Statement

2. Purpose

3. Scope

4. Definitions

5. General Provisions /Procedure

6. Roles & Responsibilities

7. Evaluation and Audit

8. References

9. Appendices

| | | | | |
|--------------------------------|---------------------------|---|---------------------------------|--------------|
| Ref No.: COR-DAM-002 | Version No.: V3 | Policy Title: Data Retention/ Destruction | Review Date: May 2021 | Page 2 of 30 |
|--------------------------------|---------------------------|---|---------------------------------|--------------|

1.0 POLICY STATEMENT

This policy sets out the obligations of The Rehab Group regarding the retention of personal data collected, held, and processed by the organisation, and the destruction of personal data in accordance with EU Regulation 2016/679 General Data Protection Regulation (“GDPR”) and national law.

Ireland: The Data Protection Act(s) 1998, 2003 (as amended) and 2018 (when enacted)

United Kingdom: Data Protection Act 1998

Poland: Personal Data Protection Act 1997 “PDPA”

The GDPR defines “personal data” as any information relating to an identified or identifiable natural person (a “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.

The GDPR also addresses “special category” personal data (also known as “sensitive” personal data). Such data includes, but is not necessarily limited to, data concerning the data subject’s race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

| | | | | |
|--------------------------------|---------------------------|---|---------------------------------|--------------|
| Ref No.: COR-DAM-002 | Version No.: V3 | Policy Title: Data Retention/ Destruction | Review Date: May 2021 | Page 3 of 30 |
|--------------------------------|---------------------------|---|---------------------------------|--------------|

In addition, the GDPR includes the right to erasure or “the right to be forgotten”. Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

- a. Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);
- b. When the data subject withdraws their consent;
- c. When the data subject objects to the processing of their personal data and the Organisation has no overriding legitimate interest;
- d. When the personal data is processed unlawfully (i.e. in breach of the GDPR);
- e. When the personal data has to be erased to comply with a legal obligation;

This policy sets out the type(s) of personal data held by the organisation, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

For further information on other aspects of data protection and compliance with the GDPR and the Data Protection Acts, please refer to the Organisation’s Data Protection Policy.

2.0 PURPOSE

The primary aim of this policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this policy aims to ensure that the organisation complies fully with its obligations and the rights of data subjects under the GDPR and the Data Protection Acts.

In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that excessive amounts of data are not retained by the organisation, this policy also aims to improve the speed and efficiency of managing data.

| | | | | |
|--------------------------------|---------------------------|---|---------------------------------|--------------|
| Ref No.: COR-DAM-002 | Version No.: V3 | Policy Title: Data Retention/ Destruction | Review Date: May 2021 | Page 4 of 30 |
|--------------------------------|---------------------------|---|---------------------------------|--------------|

3.0 SCOPE

This policy applies to all personal data held by the Rehab Group in all Rehab Group locations in Ireland, the United Kingdom and Poland and by third-party data processors processing personal data on the organisation's behalf.

Computers permanently located in the organisation's premises at all Rehab Group locations.

Laptop computers and other mobile devices provided by the organisation to its employees;

Computers and mobile devices owned by employees, agents, and sub-contractors used in accordance with the Rehab Group policies;

Physical records stored in all Rehab Group location in Ireland, the United Kingdom and Poland.

4.0 DEFINITIONS

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

| | | | | |
|-------------------------|--------------------|--|--------------------------|--------------|
| Ref No.: COR-DAM-002 | Version No.: V3 | Policy Title: Data Retention/ Destruction | Review Date: May 2021 | Page 5 of 30 |
|-------------------------|--------------------|--|--------------------------|--------------|

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Data Backup: data copied to a second location, solely for the purpose of safe keeping of that data

Data Encryption: the process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored

Data Encryption Key: an alphanumeric series of characters that enables data to be encrypted and decrypted

Regulation: a binding legislative act that must be applied in its entirety across the Union

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

5.0 GENERAL PROVISIONS / PROCEDURE

Data Subject Rights and Data Integrity

All personal data held by the organisation is held in accordance with the requirements of the GDPR and the Data Protection Acts and

| | | | | |
|-------------------------|--------------------|--|--------------------------|--------------|
| Ref No.: COR-DAM-002 | Version No.: V3 | Policy Title: Data Retention/ Destruction | Review Date: May 2021 | Page 6 of 30 |
|-------------------------|--------------------|--|--------------------------|--------------|

data subjects' rights thereunder, as set out in the organisation's Data Protection Policy.

Data subjects are kept fully informed of their rights, of what personal data the organisation holds about them, how that personal data is used as set out in the organisation's Data Protection Policy, and how long the organisation will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined by the controller).

Data subjects are given control over their personal data held by the organisation including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the organisation's use of their personal data, the right to data portability, and further rights relating to automated decision-making and profiling.

Data Destruction

Upon the expiry of the data retention periods set out below, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

- a. Personal data stored electronically (including any and all backups thereof) shall be deleted securely;
- b. Sensitive personal data stored electronically (including any and all backups thereof) shall be deleted securely;
- c. Personal data stored in hardcopy form shall be shredded. Certification of destruction is provided and assets can be tracked by serial number.
- d. Sensitive personal data stored in hardcopy form shall be shredded.
- e. Certification of destruction is provided and assets can be tracked by serial number.

Record Management

Key staff must maintain all records relevant to administering this policy in electronic form in a recognised recording keeping system.

| | | | | |
|--------------------------------|---------------------------|---|---------------------------------|--------------|
| Ref No.: COR-DAM-002 | Version No.: V3 | Policy Title: Data Retention/ Destruction | Review Date: May 2021 | Page 7 of 30 |
|--------------------------------|---------------------------|---|---------------------------------|--------------|

All records relevant to administering this policy will be maintained for a period of 5 years.

Data Retention

As stated above, and as required by law, the organisation shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out in *Appendix 3*.

When establishing and/or reviewing retention periods, the following shall be taken into account:

- The objectives and requirements of the organisation;
- The type of personal data in question;
- The purpose(s) for which the data in question is collected, held, and processed;
- The organisation's legal basis for collecting, holding, and processing that data.

If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the organisation to do so (whether in response to a request by a data subject or otherwise).

In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

| | | | | |
|--------------------------------|---------------------------|---|---------------------------------|--------------|
| Ref No.: COR-DAM-002 | Version No.: V3 | Policy Title: Data Retention/ Destruction | Review Date: May 2021 | Page 8 of 30 |
|--------------------------------|---------------------------|---|---------------------------------|--------------|

6 .0 ROLES & RESPONSILBITIES

The Organisation's Data Protection Officer(s) are;

Ireland: Margaret Murray Margaret.murray@rehab.ie
United Kingdom: Mark Bibby MBibby@RehabGroup.eu

The Data Protection Officer shall be responsible for overseeing the implementation of this policy and for monitoring compliance with this policy, the organisation's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the GDPR and other applicable data protection legislation.

The Data Protection Officer shall be directly responsible for ensuring compliance with the above data retention periods throughout the organisation.

Any questions regarding this policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Data Protection Officer.

7.0 EVALUATION & AUDIT

This policy will be reviewed on a three year basis and in conjunction with legislative amendments, Rehab Group Guidelines and organisational requirements.

8.0 REFERENCES

EU Regulation 2016/679 General Data Protection Regulation ("GDPR")

National Laws

Ireland: The Data Protection Act(s) 1998, 2003 (as amended) and 2018 (when enacted)

United Kingdom: Data Protection Act 1998

Poland: Personal Data Protection Act 1997 "PDPA"

| | | | | |
|-------------------------|--------------------|--|--------------------------|--------------|
| Ref No.: COR-DAM-002 | Version No.: V3 | Policy Title: Data Retention/ Destruction | Review Date: May 2021 | Page 9 of 30 |
|-------------------------|--------------------|--|--------------------------|--------------|

8.1 Related PPPGs

Data Protection Policy
Breach Notification & Destruction Policy

9.0 APPENDICES

Appendix 1 – List of Authors

Appendix 2 – Read & Understood

Appendix 3 – Data Retention Periods & Destruction Timelines

| | | | | |
|--------------------------------|---------------------------|---|---------------------------------|---------------|
| Ref No.: COR-DAM-002 | Version No.: V3 | Policy Title: Data Retention/ Destruction | Review Date: May 2021 | Page 10 of 30 |
|--------------------------------|---------------------------|---|---------------------------------|---------------|

Appendix 1 – List of Authors

Authors List for New/ Reviewed Policy Area

Author: Margaret Murray
Reviewer: Mark Bibby

The following names individual authors/ reviewers to this policy area.

| Division/Other | Name(s) |
|---|-----------------|
| Regional Operating Officer | Cyril Gibbons |
| Regional Operating Officer | Rachael Thurlby |
| Regional Operating Officer | Grainne Fogarty |
| Head of HR Business Partnering | Karen Fanneran |
| UK Business Support & Performance Manager | Caron Bozdugan |
| Group Financial Controller | Ray Massey |
| Head of Public Affairs | Cathy Moore |
| Data Protection Officer | Mark Bibby |

*Note that it is not obligatory for each division to be involved in a new policy/ review if the policy is not relevant; this should be decided by each division on a case-by-case basis.

Appendix 2 – Read & Understood

I have read, understand and agree to adhere to the attached Data Retention Policy, Procedure, Protocol/ SOP or Guideline:

| Print Name | Signature | Date |
|------------|-----------|------|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Appendix 3

Data Retention & Destruction Schedule

| HUMAN RESOURCES | | | | | |
|--|--|---|---------------------------------|---|---|
| <p>For logistical and functional reasons Rehab needs to operate a standardized system for data retention within HR files which means that some data is held for longer than the minimum period required by applicable legislation or recommended under Data Protection Legislation. If you would like to opt out of this system and request that each element of your file is only kept for the minimum period please contact your HR Business Partner in this regard.</p> | | | | | |
| Data Ref. | Type of Data | Purpose of Data | Review Period | Legal Limitations | Agreed Organisation Retention Period |
| Talent Acquisition | Unsolicited applications for jobs | Recruitment Process | | Not specified under legislation. | Hold for 1 year then destroy |
| Talent Acquisition | Vacancy Files - Short listing forms - Application forms & Curriculum Vitae | Recruitment Process | | Not specified under legislation. | Hold for 1 year after recruitment process has completed |
| HR Personnel file | Employee File – employee has exited the company | Employee Contract | | | Hold for 7 years after the employee has exited the company. |
| HR – Personnel files | Applications forms & Curriculum Vitae Recruitment correspondence Job Description | Employee Contract | | <i>S3.(5) Terms of Employment (Information) Acts 1994 and 2001 – a statement of particulars of the terms of employment must be kept for 1 year</i> | Retain in line with legal limitations. |
| Ref No.: COR-DAM-002 | Version No.: V3 | Policy Title: Data Retention/ Destruction | Review Date: May 2021 | Page 12 of 30 | |

| | | | | | |
|--|---|--|--|--|--|
| | <p>References</p> <p>Recruitment Medical Report</p> <p>Garda Clearance</p> <p>Proof of Professional Qualifications</p> <p>Birth Certificate</p> <p>Bank Details</p> <p>Coy of Passport/work permit for non EU Nationals</p> <p>Driving Licence</p> <p>Drivers Declaration / Insurance Information</p> <p>Contract of Employment</p> <p>PD's</p> <p>P45, TFA Certificates</p> <p>Occupational Health Assessment Reports</p> <p>Medical Certificates</p> <p>Probation Appraisal Forms</p> <p>Performance Management Forms</p> <p>Change of Circumstances Form</p> <p>Discipline Records</p> <p>Grievance Records</p> <p>Training Records</p> <p>Pension, Life Assurance & Income Protection</p> | | | <p>from termination of employment.</p> <p><i>Working Time Records: 3 years</i></p> <p><i>Protection of young Persons in Employments: 3 years</i></p> <p><i>Foreign National Employees: 5 years</i> of a period equal to the length of employment where longer than 5 years</p> <p><i>S.22 National Minimum Wage Act 2000</i> – records which show the provisions of the Act are being complied with in relation to the employee must be kept for 3 years.</p> <p><i>Collective Redundancy: 3 years</i> to show that provisions of protection of Employment Act have been complied with.</p> <p><i>Redundancy: Indefinite period</i> to ensure compliance with Redundancy Payments Acts 1967 – 2003</p> <p><i>PAYE Records</i> <i>S. 903 Taxes Consolidation</i></p> | |
|--|---|--|--|--|--|

| | | | | |
|--------------------------------|---------------------------|---|---------------------------------|---------------|
| Ref No.: COR-DAM-002 | Version No.: V3 | Policy Title: Data Retention/ Destruction | Review Date: May 2021 | Page 13 of 30 |
|--------------------------------|---------------------------|---|---------------------------------|---------------|

| | | | | | |
|-----------|---|--|--|---|--|
| | Scheme Resignation/Retirement Letter | | | <p><i>Act 1997</i> – records relating to payments to employees, must be kept for 6 years.</p> <p><i>S.886 Taxes consolidation Act 1997</i> – records which enable a person to make true tax returns must be kept for 6 years after the completion of the transactions, acts or operations to which they relate.</p> | |
| HR | Personnel - Leave Records - Annual Leave Applications - Sick Leave record including Certificates - Leave of Absence - Jury Service Leave - Study Leave - Compassionate Leave - Maternity Leave / Adoptive Leave - Parental Leave - Force Majeure Leave | Employee Contract | | Working time records / records of annual leave / records of sick leave etc: at least 3 years ¹ Carer's Leave Records: 8 years Parental Leave Records (Record of parental leave and force majeure leave taken by employees): 8 years | Retain in line with legal limitations. |
| HR | Discipline Records and letters | Employee Contract / Employee Relations | | Not specified under legislation. | Retain on personal file/ disciplinary file for the duration of the sanction (i.e. verbal warning – 6 months) then remove and destroy |

| | | | | | |
|----|--|---|--|----------------------------------|--|
| HR | Allegations /Complaints /Investigations | Employee Relations | | Not specified under legislation. | Where the complaint is If the is unfounded or investigation not warranted – hold for 12 months . Where a complaint leads to further investigation and/or an adverse finding, hold for 5 years after completion of the investigation |
| HR | Final Investigation Files | Employee Relations | | Not specified under legislation. | All manual copies of the Investigation file and any notes should be sent to Head of Employee Relations and Participation The Master manual copy will be held for a period of 5 years. All electronic data should be sent to Head of Employee Relations and Participation The Master electronic copy will be held for a period of 5 years. |
| HR | Occupational Health - Pre-employment Medical Reports - Occupational Health Assessment Reports | The purpose of occupational health & safety data is to foster a safe and healthy work | | Not specified under legislation. | Retain for 5 years after the staff member leaves/ retires (where neither the Safety Health & Welfare at Work Regulations apply, or the |

| | | | | | |
|-----------|--|-------------------|--|---|--|
| | - Other Staff Reports | environment. | | | <p>Asbestos Regulations apply) having regard to audit requirements after that date.</p> <p>Retain for 10 years where the Safety Health & Welfare at Work General Application Regulations apply, and 40 year where the Asbestos Regulations apply.</p> <p>Safety, Health and Welfare at Work Regulations 1993 "The regulations require employers to maintain records on the results of assessments, measurements of exposure and health surveillance. The records must be made available to the Health & Safety Authority, if requested."</p> |
| HR | <p>Training Files</p> <p>Training Schedules, Prospectus, programme outlines</p> <p>Staff Attendance Sheet, Evaluation Forms</p> <p>General e.g. Continuing Education Training both internal and External</p> <p>Formal Qualifications, Details f Training Courses, Course criteria,</p> | Employee Contract | | <p>Not specified under legislation.</p> <p>[Records on courses of study or training (Record of progress and results of a prescribed course of study or training): 3 years after the end of the employee's participation in the course (Regulation 3(6)(e) of the National Minimum Wage Act 2000 (Prescribed Courses of</p> | Retain for duration of employment and for 12 month on termination. |

| | | | | | |
|-----------|---|------------------|--|--|--|
| | Qualifications criteria etc. Applications for courses and sponsorship, notifications, qualifications attained. | | | Study or Training) Regulations, 2000)] | |
| HR | General I.R. and Staff Relations Records Agreement (Pay) (Other) Leave Policy & Legislation Employment Policy & Legislation Training Policy & Legislation Surveys/Reports Correspondence from Unions Individual Industrial Relations Issues Minutes of meetings Correspondence, faxes, emails Payroll Details Staff Audits | Employee Contact | | Terms of Employment (Statement of particulars of terms of employment): 1 year from termination of employment (Section 3(5) of the Terms of Employment (Information) Acts 1994 and 2001) Payroll and Wage Records (Records which show compliance with the National Minimum Wage Act 2000): 3 years from the date of their making (Section 22 of the National Minimum Wage Act 2000). PAYE Records (e.g. P11D) S.903 Taxes Consolidation Act 1997 – records relating to payments to employees must be kept for 6 years . | Retain in line with Legal Limitations. |

| DIRECTORATE OF QUALITY & GOVERNANCE | | | | | |
|-------------------------------------|---|--|--|--|--------------------------------------|
| Data Ref. | Type of Data | Purpose of Data | Review Period | Legal Limitations | Agreed Organisation Retention Period |
| Health & Safety | Accident/Incident Part X General Application Regulation 1993 (Notification of Accidents and Dangerous Occurrence to H.S.A.). | The employer is required to systematically examine the workplace and work activities to identify workplace generated hazards | | <i>Regulation 59 and 60 in Part X of the Safety Health & Welfare at Work General Application Regulations 1993</i> A record of any such incident should be retained for a period of 10 years from the date of the accident or dangerous occurrence. | Hold on file for 12 years. |
| Health & Safety | Accident/Incidents not required to be reported to the H.S.A. | | | | Hold on file for 3 years |
| Health & Safety | Asbestos European Communities (Protection of Workers)(Exposure to Asbestos) Regulations, 1989 (as amended by European Communities (Protection of Workers)(Exposure to Asbestos)(amendment) Regulations, 2000) | | | | |
| Health & Safety | Safety Statement | The Safety Statement represents a commitment by the Organisation to the safety and health of employees while they work, | The Safety Statement is reviewed on an annual basis. | Section 20, Safety Health & Welfare at Work Act, 2005. | Retain indefinitely. |

| | | | | |
|--------------------------------|---------------------------|---|---------------------------------|---------------|
| Ref No.: COR-DAM-002 | Version No.: V3 | Policy Title: Data Retention/ Destruction | Review Date: May 2021 | Page 18 of 30 |
|--------------------------------|---------------------------|---|---------------------------------|---------------|

| | | | | | |
|----------------------------|---|--|--|--|---|
| | | the safety and health of other people who might be at the workplace, including students, service users, customers, visitors and members of the public. | | | |
| Health & Safety | Safety File | This is a detailed document, which must be held by the Client for future years when repairs, maintenance & remedial works are to take place. | | Regs 6(2)(a) and 3(4) of the Safety Health & Welfare at work (Construction) Regulations 2001 and 2003 A Safety File is required for all notifiable sites under the 2006, Construction Regulations (S.I. 504, 2006). | Retain as long as premises are owned by rehab and passed on to the purchaser of property if sold. |
| Health & Safety | Inspection of Work Equipment | | | | |
| Health & Safety | Written Risk Assessment | | | | |
| | Improvement Notices and Prohibition Notices | | | | |
| Safeguarding Data | | | | | |

| FINANCE | | | | | |
|----------------------------|---|---|----------------------|--|---|
| Data Ref. | Type of Data | Purpose of Data | Review Period | Legal Limitations | Agreed Organisation Retention Period |
| Accounts Payable | Batches of Invoices and expense claim forms | Data is collected to allow the Rehab Group to collect monies owed to the Group. | | S.886 Taxes Consolidation Act 1997 – records which enable a person to make true tax returns must be kept for 6 years after the completion of the transactions, acts or operations to which they relate. Generally - accounting records to comply with Section 202 Companies Act 1990 should be retained for 6 years after the latest date to which they relate | 7 years |
| Accounts Payable | VAT Records | | | 6 years from the date of the latest transaction to which the records relate | 7 years |
| Accounts Payable | Tax Clearance Certificate | | | Not Specified | Retain until audit signed off and superseded |
| Accounts Payable | Contracts for services | | | Not Specified | Retain for duration of contract plus 7 years (where contract is under seal, retain for duration of contract plus 13 years). |
| Accounts Payable | Employee bank details | | | Not Specified | Retain until person leaves the company |
| Accounts Receivable | Debtors Listings | Data is collected to allow the Rehab Group | | The general rule is 6 years from the date of accrual of a simple contract debt (Section | 7 years |

| | | | | |
|--------------------------------|---------------------------|---|---------------------------------|---------------|
| Ref No.: COR-DAM-002 | Version No.: V3 | Policy Title: Data Retention/ Destruction | Review Date: May 2021 | Page 20 of 30 |
|--------------------------------|---------------------------|---|---------------------------------|---------------|

| | | | | | |
|-----------------------------|--|-----------------------------|---------------------------|---|---|
| | | to pay its Debtors on time. | | 11(1) Statute of Limitations 1957). Generally - accounting records to comply with Section 202 Companies Act 1990 should be retained for 6 years after the latest date to which they relate | |
| Accounts Receivable | Remittance advice | | | Not Specified | 7 years |
| Accounts Receivable | Income schedules | | | Not Specified | 7 years |
| Accounts Receivable | Receipts | | | Not Specified | 7 years |
| Accounts Receivable | Agreements – Rental, Lease, Use, Occupancy | | | Not Specified | The originals of property agreements such as leases etc. should be kept until termination, surrender or assignment, with a copy to be kept for 13 years from termination, expiration or assignment. |
| Bank Records | Paid Cheques | | Not Specified | 7 years | |
| Bank Records | Bank Reconciliations | | Not Specified | Retain until audit signed off | |
| Bank Records | Bank Statements | | Not Specified | 7 years | |
| Capital Projects | All records | | Not Specified | Retain indefinitely | |
| Financial Statements | Annual Financial Statements | | Life of Company + 6 years | Retain indefinitely if no personal data contained within | |
| Financial Statements | Final Budgetary Reports | | Not Specified | Retain until next year's audit | |

| | | | | | |
|------------------------|--|--|---|--|--|
| Mortgage assets | | | | Retain 13 years after the expiry of the Mortgage | |
| Fixed Assets | Records of Board's Properties, Sale and Purchase | | Not Specified | Retain indefinitely | |
| Fixed Assets | Assets Register | | Not Specified | Retain indefinitely | |
| Insurance Files | Policies | | Not Specified | 7 years after expiry of policy | |
| Insurance Files | Accident Reports | | Not Specified | Retain indefinitely | |
| Insurance Files | Claims correspondence | | Not Specified | Retain 7 years | |
| Other Records | Audit Reports | | Not Specified | Retain 7 years | |
| Other Records | Monthly Expenditure and Income Reports | | Taxes Consolidation Act 1997 – records which enable a person to make true tax returns must be kept for 6 years after the completion of the transactions, acts or operations to which they relate. | 6 years | |
| Other Records | Cancelled Cheques | | Not Specified | 7 years | |
| Other Records | Purchase Order Books | | Not Specified | 6 years | |
| Payroll | Listings, Payslips | | PAYE Records (e.g. P11D) S.903 Taxes Consolidation Act 1997 – records | 6 years | |

| | | | | |
|--------------------------------|---------------------------|---|---------------------------------|---------------|
| Ref No.: COR-DAM-002 | Version No.: V3 | Policy Title: Data Retention/ Destruction | Review Date: May 2021 | Page 22 of 30 |
|--------------------------------|---------------------------|---|---------------------------------|---------------|

| | | | | | |
|----------------|---|--|---|---------|--|
| | | | relating to payments to employees must be kept for 6 years. | | |
| Payroll | Pay sheets, Authorisations to deduct, tax details of staff, appointment details, pay scales, P60's, P45's | Data collection is required allow employees to be to paid on a consistent and timely basis | Employer 6 years after the end of the tax year to which they refer or for such shorter period as the Revenue Commissioners may authorise in writing to the employer | 7 years | |

OPERATIONS

Service User/Client

Individual service user files are a detailed record of all service user activities from their initial contact with the service through to their exit from the service. A list of such records is included in the retention schedule. The general principle is that:

- All children's records generated within children's services are kept indefinitely
- Adult service users' files are held for 8 years. If records in relation to adult service users availing of the Rehab services for more than 8 years as an adult do not need to be kept for a specific reason the files pre-dating the 8 year period can be summarised and the specific files destroyed in an appropriate manner.
- The files of service users who commence training services at 16 years of age need to be held for only 8 years from the date the service user turns 18.

It is the intention and obligation of the organisation to ensure that all information held on individual service users is up to date, accurate, and complete. Service users and their next of kin will also assist the organisation in updating the data.

| | | | | |
|--------------------------------|---------------------------|---|---------------------------------|---------------|
| Ref No.: COR-DAM-002 | Version No.: V3 | Policy Title: Data Retention/ Destruction | Review Date: May 2021 | Page 23 of 30 |
|--------------------------------|---------------------------|---|---------------------------------|---------------|

| Data Ref. | Type of Data | Purpose of Data | Review Period | Legal Limitations | Agreed Organisation Retention Period |
|-----------|--------------|-----------------|---------------|--|--------------------------------------|
| | | | | Child Care Act 1991 | Retain indefinitely |
| | | | | Child Care (Placement of Children in Foster Care) Regulations, 1995 | Retain indefinitely |
| | | | | Child Care (Placement of Children with Relatives) Regulations, 1995 | Retain indefinitely |
| | | | | Child Care (Placement of Children in Residential Care) Regulations, 1995 | Retain indefinitely |
| | | | | Child Care Act 1991 | Retain indefinitely |
| | | | | Child Care (Placement of Children in Foster Care) Regulations, 1995 | Retain indefinitely |
| | | | | | |

At present there is no legislation with indicates the retention period for records of adults.

Retention schedule for adult Service Users

| | | | | | |
|-----|--|--|--|---------------|----------------------|
| NLN | Application information on unsuccessful applicants | Data is collected to allow students/clients avail of our services. | | Not specified | 1 year from decision |
| | Initial Referral Letter | | | Not Specified | 7 years |
| | Service Referral Pack | | | Not Specified | 7 years |
| | Application Pack | | | Not Specified | 7 years |
| | Documentation flow chart | | | Not Specified | 7 years |
| | Initial contact sheet | | | Not Specified | 7 years |
| | Client information | | | Not Specified | 7 years |

| | | | | | |
|--|--|---|--|-------------------|---------------------------|
| | Consent forms i.e. collection of data, Compass, legal status | | | Not Specified | 7 years |
| | Assessments – F12 | The record of certification has to be kept for 16 years | | Specified by TQAS | 16 years |
| | Past and present medical details | | | Not Specified | 7 years |
| | Consent form to contact Multi-disciplinary team | | | Not Specified | 7 years |
| | Individual needs | | | Not Specified | 7 years |
| | Summary of additional needs | | | Not Specified | 7 years |
| | Individual needs check list | | | Not Specified | 7 years |
| | Risk Management process | | | Not Specified | 7 years |
| | Exist Phase Planning | | | Not Specified | 7 years |
| | Sexuality | | | Not Specified | 7 years |
| | Information on behaviours that challenge | | | Not Specified | 7 years |
| | Letter confirming service | | | Not Specified | 7 years |
| | Letter of Decline | | | Not Specified | 7 years |
| | Schedule of attendance | | | Not Specified | 7 years |
| | | | | | |
| | Resources Centres | | | | |
| | Weekly evaluation - group | | | Not Specified | 8 years (HSE requirement) |
| | Weekly evaluation - individual | | | Not Specified | 8 years |
| | Individual actions plans | | | Not Specified | 8 years |
| | Daily record sheets | | | Not Specified | 8 years |
| | Contact sheets | | | Not Specified | 8 years |

| | | | | | |
|--|--|--|--|---------------|---------|
| | Complaints | | | Not Specified | 8 years |
| | Activity Charts | | | Not Specified | 8 years |
| | Care plans | | | Not Specified | 8 years |
| | Discovery process | | | Not Specified | 8 years |
| | Service agreements | | | Not Specified | 8 years |
| | Correspondence M.D.T. Family | | | Not Specified | 8 years |
| | Notes on communication with Service users | | | Not Specified | 8 years |
| | Medical Kardex Current and previous | | | Not Specified | 8 years |
| | Declaration of self- administration of medication | | | Not Specified | 8 years |
| | Evaluation forms | | | Not Specified | 8 years |
| | Access to service users records | | | Not Specified | 8 years |
| | Attendance records | | | Not Specified | 8 years |
| | Permission to use staff/ service user images i.e. photographs/ video | | | Not Specified | 8 years |
| | Positive behaviour behavioural Support Approach | | | Not Specified | 8 years |
| | Incident reports | | | | 8 years |
| | Accident forms | | | Not Specified | 8 years |
| | CareLink as above and including: | | | | |
| | Contact details | | | Not Specified | 8 years |
| | Environment / home, community | | | Not Specified | 8 years |
| | In-depth medical needs | | | Not Specified | 8 years |
| | Who service user lives | | | Not Specified | 8 years |

| | | | | |
|--------------------------------|---------------------------|---|---------------------------------|---------------|
| Ref No.: COR-DAM-002 | Version No.: V3 | Policy Title: Data Retention/ Destruction | Review Date: May 2021 | Page 26 of 30 |
|--------------------------------|---------------------------|---|---------------------------------|---------------|

| | | | | | |
|--|---|--|--|---------------|---------|
| | Physical and sensory services as for resource centre and including | | | | |
| | List of personal belongings | | | Not Specified | 8 years |
| | Medical application form filled out by G.P. | | | Not Specified | 8 years |
| | Consent form to alternative therapies e.g. Aromatherapy, Reflexology | | | Not Specified | 8 years |
| | Assessment of activities of daily living | | | Not Specified | 8 years |
| | Waterloo score scale | | | Not Specified | 8 years |
| | Wound management chart | | | Not Specified | 8 years |
| | Contact with other services | | | Not Specified | 8 years |
| | Service user evaluations | | | Not Specified | 8 years |

| PROPERTY | | | | | |
|------------------|---------------------|---|----------------------|---|---|
| Data Ref. | Type of Data | Purpose of Data | Review Period | Legal Limitations | Agreed Organisation Retention Period |
| | Property Deeds | Title Deeds are legal documents and are required to show ownership of the property. | | Not Specified | Indefinitely |
| | Property Leases | Lease agreement describe the relationship between tenant and landlord. | | Sealed min 12 years Signed min 6 years | Indefinitely |

| | | | | |
|--------------------------------|---------------------------|---|---------------------------------|---------------|
| Ref No.: COR-DAM-002 | Version No.: V3 | Policy Title: Data Retention/ Destruction | Review Date: May 2021 | Page 27 of 30 |
|--------------------------------|---------------------------|---|---------------------------------|---------------|

| | | | | | |
|--|--------------------------|--|--|--|--------------|
| | Fire Safety Certificates | A fire safety certificate is an approval of the fire safety design incorporated into the construction of the building and ensures that the building is safe for residents. | | Maintained on premises it relates to for as long as it is in force | Indefinitely |
|--|--------------------------|--|--|--|--------------|

| REHAB ENTERPRISES | | | | | |
|--------------------------|------------------------|--|----------------------|--------------------------|---|
| Data Ref. | Type of Data | Purpose of Data | Review Period | Legal Limitations | Agreed Organisation Retention Period |
| | Contracts for Services | Contracts are in place to allow Rehab Enterprises to offer recycling services commercially | | | Indefinitely |

| IT - EMAIL- MAILMETER | | | | | |
|------------------------------|---------------------|--|----------------------|--------------------------|---|
| Data Ref. | Type of Data | Purpose of Data | Review Period | Legal Limitations | Agreed Organisation Retention Period |
| email | Unstructured Data | Email is a means of communication allowing | | Not specified. | 1 year |

| | | | | |
|--------------------------------|---------------------------|---|---------------------------------|---------------|
| Ref No.: COR-DAM-002 | Version No.: V3 | Policy Title: Data Retention/ Destruction | Review Date: May 2021 | Page 28 of 30 |
|--------------------------------|---------------------------|---|---------------------------------|---------------|

| | | | | | |
|-------------------------|-------------------|---|--|----------------|---------|
| | | employees of the Rehab Group to conduct its business. | | | |
| Mailmeter backup system | Unstructured Data | | | Not specified. | 7 years |

| | | | | |
|--------------------------------|---------------------------|---|---------------------------------|---------------|
| Ref No.: COR-DAM-002 | Version No.: V3 | Policy Title: Data Retention/ Destruction | Review Date: May 2021 | Page 30 of 30 |
|--------------------------------|---------------------------|---|---------------------------------|---------------|

The Rehab Group Personal Data Security Breach Management

Applies Jurisdiction: ALL

Division: ALL

Reference Number: COR-DAM-004

Version Number: V3

Author(s): Margaret Murray
Title: Data Protection Officer
Date: March 2018

Approver(s): Pauline Newnham
Title: Director of Quality & Governance
Date: May 2018

Signature: 

Effective From: May 2018
Review Date: May 2021

| | | | | |
|-------------------------|--------------------|------------------------------------|--------------------------|--------------|
| Ref No.: COR-DAM-004 | Version No.: V3 | Policy Title: Breach Management | Review Date: May 2021 | Page 1 of 18 |
|-------------------------|--------------------|------------------------------------|--------------------------|--------------|

Rehab Group – Personal Data Security Breach Management

Table of Contents

1. Policy Statement
2. Purpose
3. Scope
4. Definitions
5. General Provisions /Procedure
6. Roles & Responsibilities
7. Evaluation and Audit
8. References
9. Appendices

| | | | | |
|-------------------------|--------------------|------------------------------------|--------------------------|--------------|
| Ref No.: COR-DAM-004 | Version No.: V3 | Policy Title: Breach Management | Review Date: May 2021 | Page 2 of 18 |
|-------------------------|--------------------|------------------------------------|--------------------------|--------------|

Rehab Group – Personal Data Security Breach Management

1.0 POLICY STATEMENT

The Rehab Group is obliged under the EU Regulation 2016/679 General Data Protection Regulation ("GDPR") and as amended by national laws

Ireland: The Data Protection Act(s) 1998, 2003 (as amended) and 2018 (when enacted)

United Kingdom: Data Protection Act 1998

Poland: Personal Data Protection Act 1997 "PDPA"

to keep personal data safe and secure and to respond promptly and appropriately to data security breaches (including reporting such breaches to the Supervisory Authority certain cases). It is vital to take prompt action in the event of any actual, potential or suspected breaches of data security or confidentiality to avoid the risk of harm to individuals, damage to operational business and severe financial, legal and reputational costs to The Rehab Group.

2.0 PURPOSE

The purpose of this policy is to provide a framework for reporting and managing data security breaches affecting personal or sensitive personal data (defined below) held by The Rehab Group. This policy is a supplement to The Rehab Group's Data Protection Policy which affirms its commitment to protect the privacy rights of individuals in accordance with Data Protection legislation.

3.0 SCOPE

This policy applies to all users of The Rehab Group data, including: any person who is employed by The Rehab Group or is engaged by The Rehab Group who has access to The Rehab Group data in the course of their employment or engagement for administrative, research and/or any other purpose;

- members of Governing Body

| | | | | |
|-------------------------|--------------------|------------------------------------|--------------------------|--------------|
| Ref No.: COR-DAM-004 | Version No.: V3 | Policy Title: Breach Management | Review Date: May 2021 | Page 3 of 18 |
|-------------------------|--------------------|------------------------------------|--------------------------|--------------|

Rehab Group – Personal Data Security Breach Management

- any student/client of The Rehab Group who has access to The Rehab Group's data in the course of their studies for administrative, research and/or any other purpose
- individuals who are not directly employed by Rehab, but who are employed by contractors (or subcontractors) and who have access to The Rehab Group's data in the course of their duties for Rehab

These procedures apply to:

- all personal data created or received by The Rehab Group in any format (including paper records), whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically or accessed remotely
- personal data held on all The Rehab Group IT systems managed centrally by the IT Department, and locally by individuals in any Rehab Group location
- any other IT systems on which The Rehab Group's data is held or processed

4.0 DEFINITIONS

The key definitions in the GDPR in the context of data breaches are as follows:

- **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;
- **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;

| | | | | |
|-------------------------|--------------------|------------------------------------|--------------------------|--------------|
| Ref No.: COR-DAM-004 | Version No.: V3 | Policy Title: Breach Management | Review Date: May 2021 | Page 4 of 18 |
|-------------------------|--------------------|------------------------------------|--------------------------|--------------|

Rehab Group – Personal Data Security Breach Management

- **processor**: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- **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;
- **DPO**: Data Protection Officer;
- **Supervisory Authority**: an independent public authority which is established by a member state.

5.0 GENERAL PROVISIONS / PROCEDURE

A personal data security breach is any event that has the potential to affect the confidentiality, integrity or availability of personal data held by The Rehab Group in any format. Personal data security breaches can happen for a number of reasons, including:

- the disclosure of confidential data to unauthorised individuals;
- loss or theft of data or equipment on which data is stored;
- loss or theft of paper records;
- inappropriate access controls allowing unauthorised use of information;
- suspected breach of The Rehab Group's IT security and Acceptable Use policies;
- attempts to gain unauthorised access to computer systems, e.g. hacking;
- records altered or deleted without authorisation by the data "owner";
- viruses or other security attacks on IT equipment systems or networks;
- breaches of physical security e.g. forcing of doors or windows into secure room or filing cabinet containing confidential information
- confidential information left unlocked in accessible areas;
- leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information;
- Emails containing personal or sensitive information sent in error to the wrong recipient.

| | | | | |
|-------------------------|--------------------|------------------------------------|--------------------------|--------------|
| Ref No.: COR-DAM-004 | Version No.: V3 | Policy Title: Breach Management | Review Date: May 2021 | Page 5 of 18 |
|-------------------------|--------------------|------------------------------------|--------------------------|--------------|

Rehab Group – Personal Data Security Breach Management

5.1 PROCEDURE FOR REPORTING PERSONAL DATA SECURITY BREACHES

In the event of a breach of personal data security occurring, it is vital to ensure that it is dealt with immediately and appropriately to minimise the impact of the breach and prevent a recurrence.

If a member of The Rehab Group becomes aware of an actual, potential or suspected data breach of personal data, he/she must report the incident to their Manager immediately.

Report the incident immediately to the Data Protection Officer.

Complete the attached Data Security Breach Report Form (*Appendix 1*) and email it to the DPO as soon as possible.

This will enable all the relevant details of the incident to be recorded consistently and communicated on a need-to-know basis to relevant staff so that prompt and appropriate action can be taken to resolve the incident.

The DPO in conjunction with the Lead Investigator (if appointed), the Regional Operating Officer and the Head of the area affected by the breach will determine the severity of the incident using the steps as laid out in Procedure for Managing Data Security Breaches (*Appendix 2*).

6 .0 ROLES & RESPONSILBITIES

The Rehab Group's Data Protection Officers are:

Ireland & Poland Margaret Murray Margaret.murray@rehab.ie

United Kingdom Mark Bibby MBibby@rehabgroup.eu

The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, The Rehab Group's other data protection-related policies, and with the GDPR and other applicable data protection legislation.

| | | | | |
|-------------------------|--------------------|------------------------------------|--------------------------|--------------|
| Ref No.: COR-DAM-004 | Version No.: V3 | Policy Title: Breach Management | Review Date: May 2021 | Page 6 of 18 |
|-------------------------|--------------------|------------------------------------|--------------------------|--------------|

Rehab Group – Personal Data Security Breach Management

The Rehab Group shall keep written internal records of all personal data breaches.

7.0 EVALUATION & AUDIT

This policy will be reviewed every three years and in conjunction with legislative amendments, Rehab Group Guidelines and organisational requirements.

8.0 REFERENCES

EU Regulation 2016/679 General Data Protection Regulation (“GDPR”)

National Laws

Ireland: The Data Protection Act(s) 1998, 2003 (as amended) and 2018 (when enacted)
United Kingdom: Data Protection Act 1998
Poland: Personal Data Protection Act 1997 “PDPA”

8.1 Related PPGs

Data Protection Policy
Data Retention & Destruction Policy

9.0 APPENDICES

Appendix 1 - Personal Data Security Breach Report Form
Appendix 2 - Procedure for Managing Data Security Breaches
Appendix 3 – List of Authors
Appendix 4 – Read & Understood

| | | | | |
|-------------------------|--------------------|------------------------------------|--------------------------|--------------|
| Ref No.: COR-DAM-004 | Version No.: V3 | Policy Title: Breach Management | Review Date: May 2021 | Page 7 of 18 |
|-------------------------|--------------------|------------------------------------|--------------------------|--------------|

Rehab Group – Personal Data Security Breach Management

APPENDIX 1 – PERSONAL DATA SECURITY BREACH REPORT FORM

If you discover a personal data security breach, please notify your Manager/Data Champion immediately. Please complete this form and return it to the Data Protection Officer as soon as possible.

| | |
|---|--|
| Notification of Data Security Breach | |
| Date(s) of Breach: | |
| Date Incident was discovered: | |
| Name of Person Reporting Incident: | |
| Contact Details of Person Reporting Incident: | |
| Brief Description of Personal Data Security Breach: | |
| Number of Data Subjects affected – if known: | |
| Brief Description of any action since breach was discovered: | |
| Was incident report to the Office of the Data Protection Commissioner? | |
| <i>For Information Compliance Office Use Only</i> | |
| Report received by: | |
| Date: | |
| Action: | |
| Date: | |

Rehab Group – Personal Data Security Breach Management

APPENDIX 2 - PROCEDURE FOR MANAGING DATA SECURITY BREACHES

In line with best practice, the following five steps should be followed in responding to a data breach;

Step 1: Identification and initial assessment

Step 2: Containment and Recovery

Step 3: Risk Assessment

Step 4: Notification

Step 5: Evaluation and Response

Step 1: Identification and initial assessment of the incident

If a member of The Rehab Group considers that a data breach has occurred, this must be reported immediately to the staff member's Manager who will in turn notify the Department Head/ Regional Operating Officer Data Protection Officer

Ireland & Poland Margaret Murray, Roslyn Park, Beach Road, Sandymount, Dublin 4

Margaret.murray@rehab.ie 01-2057219

United Kingdom Mark Bibby,

Mbibby@Rehabgroup.eu 0044 1 200 1140

The Manager should complete part 1 of the Data Security Breach Report Form (Appendix 1) and return it to the Data Protection Officer without delay. Part 1 of the Report Form will assist the Data Protection Officer in conducting an initial assessment of the incident by establishing:

- if a personal data breach has taken place; if so:
- what personal data is involved in the breach;
- the cause of the breach;
- the extent of the breach (how many individuals are affected);
- the harms to affected individuals that could potentially be caused by the breach;
- how the breach can be contained.

| | | | | |
|-------------------------|--------------------|------------------------------------|--------------------------|--------------|
| Ref No.: COR-DAM-004 | Version No.: V3 | Policy Title: Breach Management | Review Date: May 2021 | Page 9 of 18 |
|-------------------------|--------------------|------------------------------------|--------------------------|--------------|

Rehab Group – Personal Data Security Breach Management

Following this initial assessment of the incident, the Data Protection Officer will, investigate the incident or appoint an investigator (e.g. IT Manager for IT-related incidents, etc.) and will decide if it is also necessary to appoint a group of relevant stakeholders to assist with the investigation.

Any records relating directly to an investigation will be retained by the Data Protection Officer.

The Lead Investigator (if appointed), liaising with the Data Protection Officer and the Head of the area affected by the breach, will determine the severity of the incident using the checklist in Appendix 2 and by completing part 2 of the Data Security Breach Report Form (Appendix 1) (i.e. s/he will decide if the incident can be managed and controlled locally or if it is necessary to escalate the incident to The Rehab Group Crisis Management Team).

The severity of the incident will be categorised as level 1, 2a, 2b or 3.

Level 1 classed as a Local Incident

Level 2 (a) classed as a Minor Emergency Type (A) both managed and controlled locally

Level 2 (b) classed as Minor Emergency Type (B)

Level 3 classed as a Major Emergency Escalated to Crisis Management Team which is responsible for the management and close out of the incident.

Step 2: Containment and Recovery

Once it has been established that a data breach has occurred, The Rehab Group needs to take immediate and appropriate action to limit the breach.

The Lead Investigator, liaising with the Data Protection Officer and relevant Rehab Group staff members/managers, will:

- Establish who within The Rehab Group needs to be made aware of the breach (e.g. IT Services, Property, Legal/Insurance, Communications Office) and inform them of what they are expected to do to contain the breach (e.g. isolating/closing a compromised section of the network, finding a lost piece of equipment, changing access codes on doors, etc.)

| | | | | |
|-------------------------|--------------------|------------------------------------|--------------------------|---------------|
| Ref No.: COR-DAM-004 | Version No.: V3 | Policy Title: Breach Management | Review Date: May 2021 | Page 10 of 18 |
|-------------------------|--------------------|------------------------------------|--------------------------|---------------|

Rehab Group – Personal Data Security Breach Management

- Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause (e.g. physical recovery of equipment/records, the use of back-up tapes to restore lost/damaged data).
- Establish if it is appropriate to notify affected individuals immediately (e.g. where there is a high level of risk of serious harm to individuals).
- Where appropriate (e.g. in cases involving theft or other criminal activity), inform the Gardaí.

Step 3: Risk Assessment

In assessing the risk arising from a data security breach, the relevant Rehab Group stakeholders are required to consider the potential adverse consequences for individuals, i.e. how likely are adverse consequences to materialise and, if so, how serious or substantial are they likely to be.

The information provided at Stage 1 on the Data Security Breach Report Form will assist with this stage.

The Lead Investigator and Data Protection Officer in conjunction with the Regional Operating Officer/Department Head in which the incident occurred will review the incident report to:

- Assess the risks and consequences of the breach
- Risks for individuals

- What are the potential adverse consequences for individuals?
- How serious or substantial are these consequences?
- How likely are they to happen?

Risks for The Rehab Group:

- Strategic & Operational
- Compliance/Legal
- Financial
- Reputational
- Continuity of Service Levels

| | | | | |
|-------------------------|--------------------|------------------------------------|--------------------------|---------------|
| Ref No.: COR-DAM-004 | Version No.: V3 | Policy Title: Breach Management | Review Date: May 2021 | Page 11 of 18 |
|-------------------------|--------------------|------------------------------------|--------------------------|---------------|

Rehab Group – Personal Data Security Breach Management

Determine, where appropriate, what further remedial action should be taken on the basis of the incident report to mitigate the impact of the breach and prevent repetition.

The Lead Investigator and Data Protection Officer will prepare an incident report setting out (where applicable).

- a summary of the data breach;
- the people involved in the data breach, (such as staff members, students, contractors, external clients);
- details of the information, IT systems, equipment or devices involved in the data breach and any information lost or compromised as a result of the incident;
- how the breach occurred;
- actions taken to resolve the breach;
- impact of the data breach;
- unrealised, potential consequences of the data breach;
- possible courses of action to prevent a repetition of the data breach;
- side effects, if any, of those courses of action;
- recommendations for future actions and improvements in data protection as relevant to the incident.

The incident report will then be furnished to the Regional Operating Officer (as appropriate) affected by the breach. Such Heads will request relevant staff to update the risk registers at the appropriate levels where necessary. Any significant risks will be reported to the Chief Risk Officer.

Step 4: Notification

On the basis of the evaluation of risks and consequences, the Data Protection Officer, and others involved in the incident as appropriate, will determine whether it is necessary to notify the breach to others outside The Rehab Group. For example:

- the Gardaí;
- individuals (data subjects) affected by the breach;
- the Supervisory Authority;

| | | | | |
|-------------------------|--------------------|------------------------------------|--------------------------|---------------|
| Ref No.: COR-DAM-004 | Version No.: V3 | Policy Title: Breach Management | Review Date: May 2021 | Page 12 of 18 |
|-------------------------|--------------------|------------------------------------|--------------------------|---------------|

Rehab Group – Personal Data Security Breach Management

- other bodies such as regulatory bodies, grant funders;
- the press/media;
- The Rehab Group's insurers
- bank or credit card companies
- trade unions
- external legal advisers.

In each case, the notification should include as a minimum:

- a description of how and when the breach occurred;
- what data was involved;
- what action has been taken to respond to the risks posed by the breach.

When notifying individuals, the Data Protection Officer should give specific and clear advice on what steps they can take to protect themselves, what The Rehab Group is willing to do to assist them and should provide details of how they can contact The Rehab Group for further information (e.g. helpline, website).

In accordance with the Supervisory Authority's *Personal Data Security Breach Code of Practice* all incidents in which personal data has been put at risk should be reported to the Supervisory Authority as soon as The Rehab Group becomes aware of the incident, except when the full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) and it affects no more than 100 data subjects and it does not include sensitive personal data or personal data of a financial nature. In case of doubt – in particular any doubt related to the adequacy of technological risk-mitigation measures –The Rehab Group should report the incident to the Supervisory Authority.

Any contact with the Supervisory Authority should be made through the Data Protection Officer. Initial contact with the Supervisory authority should be made by the Data Protection Officer within two working days of becoming aware of the breach, outlining the circumstances surrounding the incident. This initial contact may be by e-mail, telephone or fax and must not involve the communication of personal data. The Supervisory Authority will make a determination regarding the need for a detailed report and/or subsequent

| | | | | |
|-------------------------|--------------------|------------------------------------|--------------------------|---------------|
| Ref No.: COR-DAM-004 | Version No.: V3 | Policy Title: Breach Management | Review Date: May 2021 | Page 13 of 18 |
|-------------------------|--------------------|------------------------------------|--------------------------|---------------|

Rehab Group – Personal Data Security Breach Management

investigation based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data. In cases where the decision is made by the Lead Investigator and Data Protection Officer not to report a breach, a brief summary of the incident with an explanation of the basis for not informing the Supervisory Authority will be retained by the Data Protection Officer.

NOTE: The Communications Department should be consulted prior to any media notice being issued.

Step 5: Evaluation and Response

Subsequent to a data security breach, a review of the incident by the Data Protection Officer in consultation with the relevant stakeholders in The Rehab Group will take place to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

All data security breach reports should be sent to the Data Protection Officer who will use these to compile a central record (log) of incidents. The Data Protection Officer will report on incidents to The Rehab Group Board at least on a quarterly basis in order to identify lessons to be learned, patterns of incidents and evidence of weakness and exposures that need to be addressed.

For each serious incident, (the Lead Investigator and) Data Protection Officer will conduct a review to consider and report to the Executive Board on the following;

- What action needs to be taken to reduce the risk of future breaches and minimise their impact?
- Whether policies procedures or reporting lines need to be improved to increase the effectiveness of the response to the breach?
- Are there weak points in security controls that need to be strengthened?
- Are staff and users of services aware of their responsibilities for information security and adequately trained?
- Is additional investment required to reduce exposure and if so what are the resource implications.

| | | | | |
|-------------------------|--------------------|------------------------------------|--------------------------|---------------|
| Ref No.: COR-DAM-004 | Version No.: V3 | Policy Title: Breach Management | Review Date: May 2021 | Page 14 of 18 |
|-------------------------|--------------------|------------------------------------|--------------------------|---------------|

Rehab Group – Personal Data Security Breach Management

Appendix A – Analysis of a Data Breach

| | |
|---|---|
| Section 2: Assessment of Severity | To be completed by Lead Investigator in consultation with Regional Operating Officer/Head Of affected by the breach and DP Officer |
| Details of the IT systems, equipment, devices, records involved in the security breach: | |
| Details of information loss: | |
| What is the nature of the information lost? | |
| How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems? | |
| Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the Institute or third parties? | |
| How many data subjects are affected? | |
| Is the data bound by any contractual security arrangements e.g. to research sponsors? | |
| What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories: | |
| <p>HIGH RISK personal data</p> <ul style="list-style-type: none"> o Sensitive personal data (as defined in the Data Protection Acts) relating to a living, identifiable individual's <ul style="list-style-type: none"> a) racial or ethnic origin; b) political opinions or religious or philosophical beliefs; c) membership of a trade union; d) physical or mental health or condition or sexual life; e) commission or alleged commission of any offence, or f) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings. | |

Rehab Group – Personal Data Security Breach Management

| | |
|--|--|
| o Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as Personal Public Service Numbers (PPSNs) and copies of passports and visas; | |
| o Personal information relating to vulnerable adults and children; | |
| o Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed. | |
| o Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals. | |
| o Security information that would compromise the safety of individuals if disclosed. | |
| Category of incident (1, 2a, 2b or 3): | |
| Reported to DP Officer on: | |
| If level 2b or level 3, date escalated by Lead Investigator to the Management Team. | |

| Section 3: Action taken | To be completed by DP Officer |
|--|--|
| Incident number | |
| Report received by: | |
| On (date): | |
| Action taken by responsible officer/s : | |
| Was incident reported to Gardaí? | Yes/No If YES, notified on (date): |
| Follow up action required/recommended: | |
| Reported to DP Officer on (date): | |
| Reported to other internal stakeholders (details, dates): | |

Rehab Group – Personal Data Security Breach Management

| | |
|---|--------------------------------------|
| For use of DP Officer | |
| Notification to Data Protection Commissioner | YES/NO If YES, notified on: Details: |
| Notification to data subjects | YES/NO If YES, notified on: Details: |
| Notification to other external, regulator/stakeholder | YES/NO If YES, notified on: Details: |

Rehab Group – Personal Data Security Breach Management

Appendix 3 – List of Authors

Authors List for New/ Reviewed Policy Area

Author: Margaret Murray

Reviewer: Mark Bibby

The following names reviewers to this policy area.

| Division/Other | Name(s) |
|---|-----------------|
| Regional Operating Officer | Cyril Gibbons |
| Regional Operating Officer | Rachael Thurlby |
| Regional Operating Officer | Grainne Fogarty |
| Head of HR Business Partnering | Karen Fanneran |
| UK Business Support & Performance Manager | Caron Bozdugan |
| Group Financial Controller | Ray Massey |
| Head of Public Affairs | Cathy Moore |
| Data Protection Officer | Mark Bibby |

*Note that it is not obligatory for each division to be involved in a new policy/ review if the policy is not relevant; this should be decided by each division on a case-by-case basis.

Appendix 4 – Read & Understood

I have read, understand and agree to adhere to the attached Breach Notification Policy, Procedure, Protocol/ SOP or Guideline:

| Print Name | Signature | Date |
|------------|-----------|------|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

The Rehab Group Data Subject Access Request


Applies Jurisdiction: ALL

Division: ALL

Reference Number: COR-DAM-005

Version Number: V3

Author(s): Margaret Murray
Title: Data Protection Officer
Date: March 2018

Approver(s): Pauline Newnham
Title: Director of Quality & Governance
Date: May 2018
Signature: 

Effective From: May 2018
Review Date: May 2021

| | | | | |
|-------------------------|--------------------|---|--------------------------|--------------|
| Ref No.: COR-DAM-005 | Version No.: V3 | Policy Title: Data Subject Acc. Req. | Review Date: May 2021 | Page 1 of 12 |
|-------------------------|--------------------|---|--------------------------|--------------|

Rehab Group – Policy Title

Table of Contents

1. Policy Statement

2. Purpose

3. Scope

4. Definitions

5. General Provisions /Procedure

6. Roles & Responsibilities

7. Evaluation and Audit

8. References

9. Appendices

| | | | | |
|-------------------------|--------------------|---|--------------------------|--------------|
| Ref No.: COR-DAM-005 | Version No.: V3 | Policy Title: Data Subject Acc. Req. | Review Date: May 2021 | Page 2 of 12 |
|-------------------------|--------------------|---|--------------------------|--------------|

Rehab Group – Policy Title

1.0 POLICY STATEMENT

The GDPR details rights of access to both manual data (which is recorded in a relevant filing system) and electronic data for the data subject. This is known as a Data Subject Access Request (DSAR).

Under the GDPR, organisations are required to respond to subject access requests within one month. Failure to do so is a breach of the GDPR and could lead to a complaint being made to the Data Protection Regulator.

This policy informs staff of the process for supplying individuals with the right of access to personal data and the right of access to staff information under the General Data Protection Regulation (hereinafter called GDPR). Specifically:

All staff need to be aware of their responsibilities to provide information when a data subject access request is received. When a subject access request is received, it should immediately be reported to the Data Protection Officer to log and track each request.

Requests must be made in writing (template form is provided, but not mandatory).

The statutory response time is one month.

Requests should include the full name, date of birth and address of the person seeking access to their information. To comply with the GDPR, information relating to the individual must only be disclosed to them or someone with their written consent to receive it.

No fee can be charged for initial DSAR for all types of records, whether manual or electronic format.

2.0 PURPOSE

This policy and procedure establishes an effective, accountable and transparent framework for ensuring compliance with the requirements for the Rehab Group by the *GDPR*.

| | | | | |
|-------------------------|--------------------|---|--------------------------|--------------|
| Ref No.: COR-DAM-005 | Version No.: V3 | Policy Title: Data Subject Acc. Req. | Review Date: May 2021 | Page 3 of 12 |
|-------------------------|--------------------|---|--------------------------|--------------|

Rehab Group – Policy Title

3.0 SCOPE

These procedures apply to all users of The Rehab Group data, including: any person who is employed by The Rehab Group or is engaged by the rehab Group who has access to The Rehab Group data in the course of their employment or engagement for administrative, research and/or any other purpose;

4.0 DEFINITIONS

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

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

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

| | | | | |
|-------------------------|--------------------|---|--------------------------|--------------|
| Ref No.: COR-DAM-005 | Version No.: V3 | Policy Title: Data Subject Acc. Req. | Review Date: May 2021 | Page 4 of 12 |
|-------------------------|--------------------|---|--------------------------|--------------|

Rehab Group – Policy Title

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

5.0 GENERAL PROVISIONS / PROCEDURE

When a subject access request is received from a data subject it should immediately be reported to the Data Protection Officer who will log and track each request. If you are asked to provide information, you will need to consider the following before deciding how to respond:

Under GDPR Articles 7(3), 12, 13, 15-22 data subjects have the following rights:

- ✓ *to be informed;*
- ✓ *to access their own data;*
- ✓ *to rectification;*
- ✓ *to erasure (Right to be Forgotten);*
- ✓ *to restriction of processing;*
- ✓ *to be notified;*
- ✓ *to data portability;*
- ✓ *to object;*
- ✓ *to object to automated decision making.*

Requests must be made in writing (template form is attached, but is not mandatory). All DSARs received by email, mail, fax, social media, etc. must be processed.

The type of access you must provide and the fee you are allowed to charge may vary depending on how the records are held. It does not have to state 'subject access request' or 'data protection' to constitute a request under the GDPR.

If a request has already been complied with and an identical or similar request is received from the same individual a fee can be charged for the second request unless a reasonable interval has elapsed.

The statutory response time is one month.

Requests should include the full name, date of birth and address of the person seeking access to their information. To comply with the GDPR,

| | | | | |
|-------------------------|--------------------|---|--------------------------|--------------|
| Ref No.: COR-DAM-005 | Version No.: V3 | Policy Title: Data Subject Acc. Req. | Review Date: May 2021 | Page 5 of 12 |
|-------------------------|--------------------|---|--------------------------|--------------|

Rehab Group – Policy Title

information relating to the individual must only be disclosed to them or someone with their written consent to receive it.

Before processing a request, the requestor's identity must be verified. Examples of suitable documentation include:

Valid Passport

Valid Identity Card

Valid Driving Licence

Birth Certificate along with some other proof of address e.g. a named utility bill (no longer than 3 months old).

Fees

No fee can be charged for providing information in response to a data subject access request, unless the request is 'manifestly unfounded or excessive', in particular because it is repetitive.

If the Rehab Group receives a request that is manifestly unfounded or excessive, it will charge a reasonable fee taking into account the administrative costs of responding to the request. Alternatively, the Rehab Group will be able to refuse to act on the request.

Subject access requests made by a representative or third party

Anyone with full mental capacity can authorise a representative/third party to help them make a data subject access request. Before disclosing any information, the Rehab Group must be satisfied that the third party has the authority to make the request on behalf of the requestor and that the appropriate authorisation to act on their behalf is included (see *Appendix 3 - Data Subject Access Request Form*).

Complaints

If an individual is dissatisfied with the way the Rehab Group have dealt with their subject access request, they can complain to the Data Protection Regulator.

6.0 ROLES and RESPONSIBILITIES

Compliance, monitoring and review

The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing subject access rights at the Rehab Group rests with the Data Protection Officer.

| | | | | |
|-------------------------|--------------------|---|--------------------------|--------------|
| Ref No.: COR-DAM-005 | Version No.: V3 | Policy Title: Data Subject Acc. Req. | Review Date: May 2021 | Page 6 of 12 |
|-------------------------|--------------------|---|--------------------------|--------------|

Rehab Group – Policy Title

The Rehab Group's Data Protection Officers are:

Ireland & Poland Margaret Murray Margaret.murray@rehab.ie
United Kingdom Mark Bibby MBibby@rehabgroup.eu

All operating units' staff that deal with personal data are responsible for processing this data in full compliance with the relevant the Rehab Group policies and procedures.

Record management

Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised the Rehab Group recordkeeping system.

All records relevant to administering this policy will be maintained for a period of 5 years.

7.0 EVALUATION & AUDIT

This policy will be reviewed every three years in conjunction with any legislative amendments, Rehab Group guidelines and organisational requirements.

8.0 REFERENCES

EU Regulation 2016/679 general Data Protection Regulation ("GDPR")

National Laws

Ireland: The Data Protection Act(s) 1998, 2003 (as amended) and 2018 (when enacted)

United Kingdom: Data Protection Act 1998

Poland: Personal Data Protection act 1997 "PDPA"

| | | | | |
|-------------------------|--------------------|---|--------------------------|--------------|
| Ref No.: COR-DAM-005 | Version No.: V3 | Policy Title: Data Subject Acc. Req. | Review Date: May 2021 | Page 7 of 12 |
|-------------------------|--------------------|---|--------------------------|--------------|

Rehab Group – Policy Title

8.1 Related PPPGs

Data Protection Policy

9.0 APPENDICES

Appendix 1 – List of Authors

Appendix 2 – Read & Understood

Appendix 3 – Data Subject Access Request Form

| | | | | |
|-------------------------|--------------------|---|--------------------------|--------------|
| Ref No.: COR-DAM-005 | Version No.: V3 | Policy Title: Data Subject Acc. Req. | Review Date: May 2021 | Page 8 of 12 |
|-------------------------|--------------------|---|--------------------------|--------------|

Rehab Group – Policy Title

Appendix 1 – List of Authors

Authors List for New/ Reviewed Policy Area

The following names individual authors/ reviewers to this policy area.

| Division/Other | Name(s) |
|---|---------------------------------------|
| Regional Operating Officer | Cyril Gibbons |
| Regional Operating Officer | Rachael Thurlby |
| Regional Operating Officer | Grainne Fogarty |
| Regional Operating Officer | Jamie Lawson |
| Head of HR Business Partnering | Karen Fanneran |
| UK Business Support & Performance Manager | Caron Bozdugan |
| Barry Sweeney | Business Support & Performance Manger |
| Group Financial Controller | Ray Massey |
| Head of Public Affairs | Cathy Moore |
| Data Protection Officer | Mark Bibby |

*Note that it is not obligatory for each division to be involved in a new policy/ review if the policy is not relevant; this should be decided by each division on a case-by-case basis.

Appendix 2 – Read & Understood

I have read, understand and agree to adhere to the attached Data Subject Access Request Policy, Procedure, Protocol/ SOP or Guideline:

| Print Name | Signature | Date |
|------------|-----------|------|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Rehab Group – Policy Title

APPENDIX 3 – DATA SUBJECT ACCESS REQUEST FORM

If you want us to supply you with a copy of any personal data we hold about you, please complete this form and send it the address below. You are currently entitled to receive this information under the EU General Data Protection Regulation (GDPR). We will also provide you with information about any processing of your personal data that is being carried out, the retention periods which apply to your personal data, and any rights to rectification, erasure, or restriction of processing that may exist.

The information you supply in this form will only be used for the purposes of identifying the personal data you are requesting and responding to your request.

1 Please send your completed form and proof of identity to: [Address]

2 Section 1: Details of the person requesting information

| | |
|------------------------|--|
| Your full name: | |
| Your address: | |
| Your telephone number: | |
| Your email address: | |

3 Section 2: Are you the data subject?

Please tick the appropriate box.

YES: I am the data subject. I enclose proof of my identity (see below). Please proceed to Section 4.

NO: I am acting on behalf of the data subject. I have enclosed the data subject's written authority and proof of the data subject's identity and my own identity (see below). Please proceed to Section 3.

To ensure we are releasing data to the right person we require you to provide us with proof of your identity and of your address. Please supply us with a photocopy or scanned image (do not send the originals) of one of both of the following:

- 1) **Proof of Identity.** We need one of the following: passport, photo driving license, national identity card, birth certificate.
- 2) **Proof of Address.** We need one of the following: utility bill, bank statement, credit card statement (no more than 3 months old); current driving license; local authority tax bill.

If we are not satisfied you are who you claim to be, we reserve the right to refuse to grant your request.

| | | | | |
|-------------------------|--------------------|---|--------------------------|---------------|
| Ref No.: COR-DAM-005 | Version No.: V3 | Policy Title: Data Subject Acc. Req. | Review Date: May 2021 | Page 10 of 12 |
|-------------------------|--------------------|---|--------------------------|---------------|

Rehab Group – Policy Title

- To whom your personal data are disclosed
- The source of your personal data

7 Section 6: Disclosure of CCTV images

If the information you seek is in the form of video images captured by our CCTV security cameras, would you be satisfied with viewing these images?

- YES
- NO

8 Section 7: Declaration

Please note that any attempt to mislead may result in legal action.

I confirm that I have read and understood the terms of this Data Subject Access Request Form and certify that the information given in this application to the Rehab Group is true. I understand that it is necessary for the Rehab Group to confirm my / the data subject's identity and it may be necessary to obtain more detailed information in order to locate the correct personal data.

.....
Signature

.....
Date

9 Attachments:

I am enclosing the following copies as proof of identity:

.....
.....
.....
.....
.....
.....
.....
.....