CARI DATA PROTECTION POLICY

September 2019

Change history

Date	Version	Created by	Description of change

Table of Contents

Purpose and scope for users

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of CARI. This includes obligations in dealing with personal data, in order to ensure that CARI complies with the requirements of the relevant Irish legislation, namely the Irish Data Protection Act (1988), and the Irish Data Protection (Amendment) Act (2003) and the General Data Protection Regulation (GDPR) that came into effect on the 25th May 2018.

This policy applies to all personal data collected, processed and stored by CARI in relation to data subjects who engage with CARI in the course of its activities. The policy covers both personal and sensitive personal data held in relation to data subjects by CARI. The policy applies equally to personal data held in manual and automated form.

All personal and sensitive personal data will be treated with equal care by CARI. Both categories will be equally referred to as personal data in this policy, unless specifically stated otherwise.

Reference documents

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)
2. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
3. Data Protection Act 2018
4. Data Protection Act 1988 REVISED Updated to 25 May 2018
5. Personal Data Security Breach Report Form
6. Employee Handbook, Section 6: Organisational Policies
7. CARI Therapy Clinical Practice Policies book
8. CARI Privacy Policy
9. CARI Financial Policy

Definitions

Competent Authority

A competent authority is: (a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or (b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Supervisory Authority

An independent public authority which is established by a Member State pursuant to Article 51 of the EU GDPR.

Personal Data

Personal data is 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

Controller

This is 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.

Processor

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

Processing

Processing is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Protection Officer

The Data Protection Officer is a person designated to act as a data protection officer of a controller or processor for the purposes of Articles 37 to 39 of the GDPR.

Establishment

Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

Personal Data Breach

Personal data breach is defined as 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.

Pseudonymise

Pseudonymise means to process personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Anonymization

Anonymization means data that is rendered anonymous in such a way that the data subject is not or no longer identifiable.

Right of Access

A data subject's right to obtain confirmation from a controller whether the controller holds any personal data relating to that individual and, if it does, to obtain access to that personal data and information in relation to the processing.

Right to Rectification

A data subject's right to require a controller to rectify any inaccuracies in personal data relating that individual.

Right to be Forgotten

A data subject's right to require a controller to delete personal data relating to that individual in certain circumstances.

Right to Restrict Processing

A data subject's right to require a data controller to restrict processing of personal data relating to that individual in certain circumstances.

Right to Data Portability

A data subject's right to receive personal data concerning that individual, which that individual provided to a controller, in a structured, commonly used and machine-readable format and the right to require the controller to transmit that personal data to another controller at the request of the individual in certain circumstances.

Right to Object

A data subject's right to object to processing of personal data relating to that individual, where the processing is based on certain legal grounds for processing.

Right Against Automated Decision Making

A data subject's right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, except in limited circumstances.

Special Categories of Personal Data

This means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Third party

'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

CARI

CARI is committed to protecting the privacy of those who use our services either through our website through our fundraising function or through our clinical and support services in CARI and complying with our obligations under the Data Protection Acts 1988 and 2003 (the Acts) and the General Data Protection Regulation (GDPR). CARI care about the security and privacy of the personal data it processes. In the course of its daily organisational activities, CARI acquires, processes and stores personal data in relation to:

1. Employees of CARI
2. Clinical clients of CARI (therapeutic and support services)
3. Third party service providers engaged by CARI
4. Financial donors of CARI
5. Fundraising supporters of CARI
6. CARI website

In accordance with the relevant Data Protection Legislation, the above data must be acquired and managed fairly. Not all staff members will be expected to be experts in Data Protection Legislation. However, CARI is committed to ensuring that its staff have sufficient awareness of the legislation in order to be able to anticipate and identify a Data Protection issue, should one arise. In such circumstances, staff must ensure that the Data Compliance Officer is informed, so that appropriate corrective action can be taken.

This policy provides the guidelines for how and why CARI processes personal data as well as the procedure to follow in order to address the various rights of the data subject.

Basic principles regarding personal data processing

The General Data Protection Regulation has set out fundamental principles governing the processing of personal data. There are six Data Protection Principles that all Controllers must follow according to Article 5 GDPR when processing personal data.

1. Lawfulness, fairness and transparency

Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the data subject

2. Purpose limitation

Personal Data must be 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.

3. Data minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Accuracy

Personal Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5. Storage period limitation

Personal Data must be 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

6. Integrity and confidentiality

Personal Data must be 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.

Accountability

The Data Controller (CARI) shall be responsible for and be able to demonstrate compliance with the above.

CARI Data Retention

CARI processes and stores different types of personal data:

1. Employee Data
2. Clinical client Data

3. Donor/fundraising Data

GDPR does not set out specific retention periods within its legislation however it states that personal data may only be kept in a form which permits identification of the individual for no longer than is necessary for the purposes for which it was processed.

There are specific retention periods set out in law however for data retention through its employer function. CARI's retention policy for employee data can be found in Section 6 of the CARI Employee Handbook.

Therapy and Child Accompaniment Support Services notes are kept for 7 years after client is 18. Helpline calls are retained for 7 years. The retention periods for the clinical and support services have been decided by CARI and are set out in the CARI Therapy Clinical Practice Policies book.

Financial files should be retained by CARI until after the annual audit. They may then be archived and must be retained for six years, further information on financial records is outlined in the CARI Financial Policy.

Disclosure to third parties

In the course of its role as Data Controller, CARI may engage Data Processors to process Personal Data on its behalf. In such a case, a formal written contract is in place with the processor. This contract will outline their obligations in relation to the Personal Data, the specific purpose or purposes for which they are engaged, and the understanding that they will process the data in compliance with the Irish Data Protection legislation.

Rights of the Data Subject

Rights of Data Subjects Individuals have the following rights over the way CARI process their personal data:

Right of Access by the data subject

Please see 'Rights of Access by Data Subjects' below.

Right of rectification

Individuals have the right to have inaccuracies in personal data that CARI hold about them rectified.

Right to erasure (right to be forgotten)

Individuals have the right to have their personal data deleted where CARI no longer have any justification for retaining it subject to exemptions such as the use of pseudonymised data for scientific research.

Right to restriction of processing

Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, CARI is permitted to store the personal data, but not use it. An individual can make a request for restriction verbally or in writing and CARI must respond within one calendar month.

Right to data portability

Where it is technically feasible individuals have the right to have a readily accessible machine-readable copy of their data transferred or moved to another data controller where CARI are processing their data based on their consent and if that processing is carried out by automated means.

Right to object

Individuals have the right to object to processing or restrict the processing of their personal data if:

1. The processing is based on public interest or in order to pursue a legitimate interest
2. The personal data was processed unlawfully;
3. You need the personal data to be deleted in order to comply with a legal obligation;

Rights of Access by Data Subjects

Employee data

Please see the CARI Employee Handbook, Section 6: Organisational Policies for the policy of accessing data as a CARI employee.

Service User Data

CARI takes very seriously its obligations as a data controller as set out in the under the Data Protection Acts 1988 and 2003 (the Acts) and the General Data Protection Regulation (GDPR).

Data subjects whose personal data is held by CARI are entitled to ask CARI and receive confirmation as to whether personal data concerning them is being processed. Where that is the case, data subjects are entitled to access the personal data as well as the following information concerning their data:

1. The purposes of processing
2. The categories of personal data concerned

3. The recipients or categories of recipients to whom personal data has been or will be disclosed
4. Where possible the envisaged period for which personal data will be stored, or if not possible, the criteria used to determine that period
5. The existence of the right to request from CARI rectification or erasure of personal data or restriction of processing personal data concerning the data subject or to object to such processing
6. The right to lodge a complaint with the Data Protection Commissioner
7. Where the personal data is not collected from the data subject, any available information regarding the sources
8. The existence, if any, of automated decision-making (including profiling) being operated on the data subject's data
9. If personal data is transferred to a third country the appropriate safeguards pursuant to the GDPR relating to such transfer

Form of the Request

A Subject Access Request can be made by writing to CARI, 110 Lower Drumcondra Road, Drumcondra, Dublin 9, clearly stating a Subject Access Request (SAR).

CARI may ask the data subject to provide evidence of their identity. This is to make sure that personal information is not given to the wrong person. When CARI are satisfied with this criterion it will be in a position to commence the work involved in responding to the request.

CARI will respond to the access request within one month of receiving the request. Depending on the complexity of the request and the number of requests CARI may have to extend the one-month period by two months. If CARI needs to extend this time it will inform the data subject of this and give the data subject the reason(s) for the delay in responding, within one month of receiving the request.

There is no fee payable by the data subject to make an access request. However, if CARI believed that a request is manifestly unfounded or excessive CARI may either charge a fee considering its administrative costs in dealing with the request(s) or refuse to act on the request(s).

Please note that Under section 5, Article 23 of the Regulation CARI has the right to restrict the rights of Article 15 Right of Access of Data Subject if CARI determine that it is a necessary and proportionate measure in order to safeguard and protect the data subject or the rights and freedoms of others.

Communicating with the Data Subject

CARI will communicate directly with the data subject once a valid subject access request has been received. This contact may help the data subject specify the exact information they wish to receive.

If the data subject requests a copy of everything CARI holds about them, then it will fulfil a complete and exhaustive search of all relevant data in CARI.

Systems and Manual files Search

Unless there is a legitimate option to reduce the scope of the request, a search of all databases and all relevant filing systems (manual files) which are relevant under the GDPR will be carried out throughout CARI.

Restrictions Following Receipt of a Request

Compliance with GDPR and related legislation is not intended to interfere with the normal running of CARI business, and following receipt of a valid request, CARI are permitted to make changes to the requested information in the normal course of operation provided no changes are made because of the request itself. This includes the correction of incorrect data.

Third Party Data

Once the information has been collected, CARI will consider our obligations to other data subjects. The person(s) preparing our response will consider the rights of third parties and any obligations of confidentiality which may apply, in addition to any relevant exemptions under GDPR. Where the identity of third parties would be disclosed in data which related to the data subject, CARI may either blank out (redact) that data to protect the privacy and confidentiality of such third parties or may provide the data subject with an extract from the data instead of the original sources material.

Exemptions

Some material is exempt from inclusion in the response to a subject access request. This includes the content of negotiations with the data subject and information which is subject to legal professional privilege. It also includes information relating to ongoing professional investigation or determination processes. If CARI are negotiating with the data subject at the same time, they make a subject access request, CARI do not have to reveal requested information if to do so would likely to prejudice those negotiations. Once the negotiations are complete and put into effect, the file becomes subject to GDPR.

Emails are subject to subject access, as are archived computerised and manual data held in a relevant filing system.

Where personal data contains health information, there may be a duty on CARI to consult an appropriate health professional before information can be disclosed. This is to avoid disclosing information about adverse health conditions to a data subject where the disclosure may be harmful

or distressing to the data subject or another person. This does not apply where the data subject already had access to, or supplied, the information.

Form of Response

CARI will provide the data subject with any relevant data in response to a subject access request in electronic format. If the data subject does not wish to receive our response to their request by email, please let us know in advance. Once our response to the subject access request has been finalised, CARI will make a full copy of the material to be retained for its own reference. This record will be used as a reference should there be any dispute as to the content or timeliness of CARI's response provided to the data subject. It will be retained for seven years.

Organisation and responsibilities

CARI holds the overall responsibility for ensuring compliance with the Data Protection Acts. However, all employees who process personal data in the course of their employment are also responsible for ensuring compliance with the Data Protection Acts.

CARI will provide support, assistance, advice and training to all relevant departments and staff to ensure they are in a position to comply with the legislation. CARI's Data Compliance Officer will assist CARI and its staff in complying with the Data Protection legislation.

Specifically, the following roles and responsibilities apply in relation to this policy:

CARI Board of Trustees

- CARI Board of Trustees are responsible for reviewing and approving this policy.

CARI Management

- Read and understand this policy.
- The CARI Management Team is responsible for ensuring compliance with the Data Protection Acts and this policy in their respective areas of responsibility
- All responsibilities pertaining to CARI Staff also apply to CARI Management.

CARI staff/volunteers

- Read and understand this policy
- Must complete relevant training and awareness activities provided by CARI to support compliance with this policy.
- Should take all necessary steps to ensure that no breaches of information security result from their actions.

- Must report all suspected and actual data security breaches to the CARI Data Compliance Officer, so that appropriate action can be taken to minimise harm.
- Must inform CARI of any changes to information that they have provided to CARI in connection with their employment (e.g. changes of address, back account details).

CARI Data Compliance Officer

- Will be a point of contact for the organisation regarding Data Protection.
- Bring Data Protection security matters to the attention of CARI staff.
- Provide training and awareness to all those involved in processing data on behalf of CARI to ensure processing is kept compliance
- Provide training and awareness to staff on Data Protection and what it means for the organisation
- Serve as the point of contact with the relevant Supervisory Authority
- Provide advice and guidance to all staff and management of CARI
- Participating in training in Data Protection/IT security where appropriate.

Supervisory authority

The supervisory authority for any issues regarding how CARI manages personal data is The Data Protection Commissioner. This Office can be contacted at the following address: Dublin Office
21 Fitzwilliam Square, Dublin 2, D02 RD28, Ireland. The contact phone number is 1890 252 231 and the website is www.dataprotection.ie.

Response to personal data breach incidents

An obligation relating to data breach notification should be reflected in the terms of engagement between CARI and its Service Users so that both parties will know to react immediately to any data breach that occurs as soon as they become aware of it.

Where there is a risk to data subjects and reporting is required CARI must do so without delay and no later than 72 hours after having become aware of the data breach. When reporting a data breach, CARI should:

- Describe in clear and plain language the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
- Communicate the name and contact details of the Data Compliance Officer or other contact point where more information can be obtained;

- Describe the likely consequences of the personal data breach;
- Describe the measures taken or proposed to be taken CARI to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
- CARI shall document on its Personal Data Security Breach Report Form any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the DPC to verify compliance with Article 33.

The communication to the data subject shall not be required if:

- CARI has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- CARI has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
- it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

If CARI has not already communicated the personal data breach to the data subject, the DPC, having considered the likelihood of the personal data breach resulting in a high risk, may require CARI to do so.

Right to complain

If a data subject is unhappy with how CARI has dealt with their data, the data subject can contact us at cass@cari.ie outlining their concern and CARI will respond immediately.

If the person remains unsatisfied it is their right to bring their concerns to the Data Protection Commissioner. The contact details are as follows; The Data Protection Commissioner, Dublin Office, 21 Fitzwilliam Square, Dublin 2, D02 RD28. 1890 252 231. www.dataprotection.ie.

Audit and Accountability

The CARI Board of Management is responsible for how well the CARI Departments and the organisation implement this policy.

Security and Record Management

Security

CARI will ensure that appropriate technical and organisational measures are in place, supported by regular monitoring of data processing, to ensure a high level of security for personal and confidential data. CARI will ensure a secure environment for information held both manually and electronically.

Record Management

Record management refers to a set of activities required for systematically controlling the creation, distribution, use, storage and disposal of recorded information maintained as evidence of service provision. Good record management practices ensure not only record quality, but that personal data is only kept for as long as necessary for its original purpose and help support data minimisation. CARI is committed to implementing and monitoring robust records management practices.

Record keeping practices for the therapeutic and support services of CARI are outlined in the CARI Therapy Clinical Practice Policies book.

Record keeping policy for CARI employee data is outlined in Section 6 of the CARI Employee Handbook.

Financial files should be retained by CARI until after the annual audit. They may then be archived and must be retained for six years, further information on financial records is outlined in the CARI Financial Policy.

Validity and document management

This Policy is valid from 27th February 2020. It will be reviewed regularly considering any legislative or other relevant developments.