StepIn policy on General Data Protection

Document reference number	GDPR	Document developed by	Brian Feeney
Revision number		Document approved by	Board of Directors
Approval date		July 26, 2018	
Revision date	This policy will be reviewed at least every two years or immediately on changes of relevant legislation	July 2020	

1. Introduction

StepIn is committed to fulfilling General Data Protection Regulations in its operational activities. GDPR strengthens the rights of individuals and increases the obligations on organisations such as StepIn to have good, valid reasons for holding personal information. StepIn is committed to keeping information secure; responding to any requests and reporting any breaches of security. It fulfils these commitments in the following ways:

2. Consent for collecting data

Personal data is any information relating to an individual such as a person's name, address, age, photo, PPS number, bank details, medial records.

StepIn will comply with GDPR requirement that consent is freely given for any personal data. Consent will be recorded so it can be verified. Where existing data has no record of consent, StepIn will contact to verify consent. Collection of data will be for an explicit and legitimate purpose.

3. Explicit and legitimate purposes

StepIn will only collect personal data for explicit and legitimate purposes. These purposes may be summarised as follows:

- **Consent**: A person has clearly and willingly agreed to provide the information. StepIn will clearly explain the reason(s) for requesting the information.
- **Contract**: It's necessary for the performance of a contract.
- **Legal obligation:** Processing is necessary to comply with a legal obligation
- **Vital interests:** It is necessary to protect the vital interests of the "data subject."
- **Public interest:** Processing is necessary for the performance of a task in the public interest or in the interest of an official, regulatory or statutory authority, which is vested in the controller (for example where StepIn is acting as an agent for the HSE).
- **Legitimate interest:** The process is necessary for the legitimate interests of StepIn (except when overridden by the rights and freedoms of the individual).

4. Security

StepIn will put in place procedures and practices to maximise the security of information it holds. Staff will be made aware of their data protection responsibilities - including the need for confidentiality. This will be done in a number of ways, including supervision, training, guidance notes and policies
Staff are advised that they:

- Obtain and process information fairly
- Keep it for specified and lawful purpose(s)
- Process it only in ways compatible with the purposes for which it was given
- Keep it safe and secure
- Keep it accurate and up to date
- Ensure it is adequate, relevant and not excessive.
- Retain it no longer than is necessary for the specified purpose
- Give a copy of personal data to any individual on request.

The safety and security of information is detailed in full in StepIn's Data Protection Policy.
In brief, StepIn will do the following:

- Ensure access to StepIn computers and manual files are restricted to authorised staff only.
- Restrict access to personal/ sensitive information on a "need-to-know" basis.
- Password protect StepIn computer systems.
- Keep information on screens hidden from callers to StepIn's offices
- Have a back-up procedure in operation.
- Ensure sensitive printouts are shredded and all waste papers disposed of carefully.

5. Recording collection of data

StepIn will record a person's consent and the rationale for seeking consent. The consents will be logged by StepIn staff. The Supported Living coordinator is responsible for ensuring StepIn meets compliance on records of data.

4. Timeframes for retention of data

StepIn implements the following time frames for retention of data:

- Health and safety — records of major acts and incidents — 10 years
- Recruitment — records and interview notes of unsuccessful applicants — 12 months
- Employees — contracts after termination — seven years
- Employees — records of employee tax payments — six years
- Health and safety — general — seven years
- Tax and accounts — accounting records of transactions, company accounts — six years.

Outside of the above timelines, “data will not be kept for longer than is necessary for that purpose or those purposes.” More time may be needed if legal action is threatened.

5. Registration

Some organisations are exempt from registering with the Data Protection Commissioner. The following two exemptions indicate StepIn does not need to register:

- Organisations that only process manual data (unless the data has been prescribed by the Commissioner as requiring registration);
- Organisations that are not established or conducted for profit and that are processing data related to their members and supporters and their activities.

6. Data breach

StepIn is obliged to report a data breach. It will give a first notification within 24 hours to the Data Protection Commission. If not all information is to hand, a second notification will be made within three days of the first. StepIn’s Data Breach Notification procedure and form is appended to this policy.

7. Accessing Personal Information

There are two deadlines for responding to access requests — 21 days and 40 days. The longer response time is for **“copies”** of the information.

Under **Section 3** of the Data Protection Acts, a person has a right to find out, free of charge, if an individual or an organisation holds information about you. They also have a right to be given a description of the information and to be told the purpose(s) for holding your information.
The request must be made in writing. StepIn must send the information within 21 days.

Under **Section 4** of the Data Protection Acts, 1988 and 2003, a person has a **right to obtain a copy**, clearly explained, of any information relating to them kept on computer or in a structured manual filing system or intended for such a system by any entity or organisation.

StepIn requests a fee of €5 for handling a request. Once the request has been received StepIn must give the information within 40 days. StepIn’s Data Access procedure and request form is appended to this policy.

Addendum1.

StepIn Data Breach Notification Form

StepIn is obliged to report a data breach. This form outlines what to do; the information that we need to provide; the timelines; and where it needs to be sent. Examples of what constitutes a data breach are set out in StepIn’s Data Protection Advice sheet. Also refer to dataprotection.ie for further advice and information.

An obligation to report within 24 hours

A first notification must be made to the Data Protection Office on this form no later than 24 hours after the first detection of the data breach.

If you have all the information to hand at this stage, you may fill out both sections 1 and 2 of the form.

If you do not have all the necessary information to hand at the time of the first notification, a second notification must be made within 3 days of the first notification, on section 2 of the form.

When submitting a second notification, please complete Questions 1-3 again and Questions 4-8 if there is any change to the information. If there is no change to your responses to questions 4 to 8 from your initial notification, simply enter "as initial notification".

Data Breach Notification Form

Section 1

1. Name of provider

2. Contact details

3. Indicate if this is a first or second notification

4. Indicate both the date and time when the incident took place and the date and time when the incident was detected by the provider.

5. Indicate the circumstances surrounding the breach.

6. Indicate the nature and content of the personal data.

7. Indicate the technical and organisational measures you are applying to secure the affected data.

8. Indicate if you use other providers to deliver part of the electronic communications service to your subscribers. If the breach was related to the service provided by these other providers, please indicate if they notified you of the data security breach. At the end of Section 1 you will be given an option either to submit the form as an initial notification or to proceed to section 2 to make a full notification, if you have the information available to you at this time. If you submit you will receive an automated email as an initial acknowledgment.

How to Notify Data Protection Commissioner

E-Mail - dpcbreaches@dataprotection.ie

Phone - 1890 252231(lo-call); 00 353 (0) 57 8684800

Fax- 00 353 (0) 57 8684757

SECTION 2

Further Information on the data breach.

9. Give a summary of the incident that caused the data breach, including the physical location and the storage media involved.

10. Indicate the number of subscribers or individuals concerned.

11. Describe the potential consequences and potential adverse effects on subscribers/ individuals.

12. Describe what action you have taken to help mitigate any potential adverse affects to the affected individuals. *Possible additional notification to subscribers/individuals.*

13. If you have already notified subscribers/individuals, please give the content of the notification.

14. If you have already notified subscribers/individuals, please indicate the means used to notify the breach to subscribers/individuals (e.g. individual notifications- email, letter or phone call, media announcements etc).

15. Indicate the number of subscribers/individuals notified. *Possible cross-border issues*

16. Indicate if the breach has involved subscribers/individuals in other Member States.

17. Indicate if you have notified other competent national authorities. If you have notified other competent national authorities, please indicate which authorities you have notified.

How to Notify Data Protection Commissioner

E-Mail - dpcbreaches@dataprotection.ie

Phone - 1890 252231(lo-call); 00 353 (0) 57 8684800

Fax- 00 353 (0) 57 8684757

Addendum 2.

Dealing with a data access request

Every individual about whom StepIn keeps personal information on computer or in a relevant filing system, has a number of rights under the Acts, in addition to the Right of Access. These include the right to have any inaccurate information rectified or erased; to have personal data taken off a direct marketing or direct mailing list and the right to complain to the Data Protection Commissioner.

An application to StepIn for access to personal information will be dealt with by the Supported Living Coordinator. He or she will record the date the application is received by StepIn and notify the chairperson.

An application for access to personal information must be in writing, giving any details which might be needed to help identify him or her and locate all the information StepIn may keep about him/her. The individual must also pay an access fee of €5.

What StepIn must do in response to a request to access personal data

Supply the information to the individual within 40 days of receiving the request. Note that, having received the access request, StepIn cannot change or delete the personal data which it holds.

Provide the information in a form which will be clear to the ordinary person (any codes must be explained).

Ensure that StepIn gives personal information only to the individual concerned (or someone acting on his or her behalf and with their authority). For instance, StepIn normally would not provide such information by phone.

If there is no information on computer or in a relevant filing system about the individual making the request, StepIn should tell them so within the 40 days.

StepIn is not obliged to refund any fee it may have charged for dealing with the access request should it find there is not, in fact, any data. However, the fee must be refunded if StepIn does not comply with the request, or if StepIn has to rectify, supplement or erase the personal data concerned.

What StepIn must supply

Under section 4 of the Data Protection Acts, on making a written request to StepIn, any individual about whom there is personal information on computer or in a relevant filing system is entitled to:

(a) a copy of the data,
(b) a description of the purposes for which it is held,
(c) a description of those to whom the data may be disclosed and
(d) the source of the data unless this would be contrary to public interest

Exceptions or limitations on right of access

- There are some exceptions or limitations on the right of access to information. For instance, the right of access does not include a right to see personal data about another individual, without that other person's consent. This is necessary to protect the privacy rights of the other person.
- Where personal data consists of expressions of opinion about the data subject by another person, the data subject has a right to that expression of opinion, except where that expression of opinion was given in confidence.
- The obligation to comply with an access request does not apply where it is impossible to provide the data or where it involves a disproportionate effort.

Sample response form for data access request

A sample form for response to an access request is given below. This may be used or, alternatively, the response may be given in letter format. The letter response should include details of the applicant; the date of application; summary of the copies of data enclosed; a description of the purposes for which it is held; a description of those to whom the data may be disclosed; the source of the data; receipt for application fee.

If StepIn does not hold any information, it is sufficient to respond in writing stating this.

Data Access Request Form

StepIn Supported Living Networks
Cherry House, Comans Park,
Roscommon.
Registered Charity Number 20105525

Date:

Dear

In response to your request for access to personal information held by StepIn, the following information is enclosed and details provided.

Yours sincerely,

1. Name of data access applicant

2. Contact details of applicant

3. Summary of information request

4. Summary of copies of information provided by StepIn

5. Description of the purposes for which it is held

6. Description of those to whom the data is disclosed

7. The source of the data

Details of StepIn staff member providing details

NAME:

E-MAIL:

PHONE