A Little Lifetime Foundation Data Protection Policy

A Little Lifetime Foundation regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

Purpose

The purpose of this document is to provide a policy regarding the data protection obligations of A Little Lifetime Foundation (ALLF). It defines how we manage responsibilities as a Board, volunteers and employees under the General Data Protection Regulations Act 2018 (GDPR). ALLF intends to ensure that personal information is treated lawfully and correctly.

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of Europe 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.

ALLF is a data controller with reference to the personal data which it manages, processes and stores. ALLF therefore has obligations under the Data Protection legislation, which are reflected in this document.

For the purposes of this policy, data includes both automated and manual data.

- Automated data means data held on computer, or stored with the intention that it is processed on computer.
- Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.

In the course of its daily organisational activities, ALLF acquires and stores personal data in relation to living individuals. To that extent, in accordance with Irish Data Protection legislation, this data must be acquired and managed fairly.

ALLF is committed to ensuring that all staff members and volunteers 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, they must ensure that the Data Protection Officer (DPO) is informed, in order that appropriate corrective action is taken.

ALLF will ensure that data is collected within the boundaries defined in this policy. This

applies to data that is collected in person, or by completing a form.

When collecting data, ALLF will ensure that the Individual/Service User:

a) Clearly understands why the information is needed

b) Understands what it will be used for and what the consequences are should the Individual/Service User decide not to give consent to processing

c) Has received sufficient information on why their data is needed and how it will be used

The Data Protection Rules

The following key rules are enshrined in Irish legislation and are fundamental to ALLF's data protection policy.
In its capacity as data controller, ALLF ensures that all data shall:

1. Be obtained and processed fairly and lawfully
For data to be obtained fairly, the data subject will, at the time the data are being collected, be made aware of:

- The identity of the data controller (ALLF);
- The purpose(s) for which the data is being collected;
- The person(s) to whom the data may be disclosed by the data controller;
- Any other information that is necessary so that the processing may be fair.

ALLF will meet this obligation in the following way:

- The informed consent of the data subject will be sought before their data is processed;
- Processing of the personal data will be carried out only as part of ALLF's lawful activities, and it will safeguard the rights and freedoms of the data subject;

2. Be obtained only for one or more specified, legitimate purposes
ALLF will obtain data for purposes that are specific, lawful and clearly stated. A data subject will have the right to question the purpose(s) for which ALLF holds their data, and it will be able to clearly state that purpose or purposes.

3. Not be further processed in a manner incompatible with the specified purpose(s)
Any use of the data by ALLF will be compatible with the purposes for which the data was acquired.

4. Be kept safe and secure
ALLF will employ high standards of security in order to protect the personal data under its care. Information and records relating to service users will be stored securely and will only be accessible to authorised staff and volunteers. Access to, and management of, records is limited to those staff members who have appropriate authorisation and password access. In the event of a data security breach affecting the personal data being processed on behalf of the data controller, the relevant third party processor will notify the data controller without undue delay.

5. Be kept accurate, complete and up-to-date where necessary
ALLF will:

- Ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy;
- Conduct periodic reviews and audits to ensure that relevant data is kept accurate and up-to-date.
- *Conduct regular assessments in order to validate the need to keep certain personal data.*

6. Be adequate, relevant and not excessive in relation to the purpose(s) for which the data were collected and processed
ALLF will ensure that the data it processes in relation to data subjects are relevant to the purposes for which those data are collected. Data which are not relevant to such processing will not be acquired or maintained.

7. Not be kept for longer than is necessary to satisfy the specified purpose(s)
Once the respective retention period of the data we hold has elapsed, ALLF undertakes to destroy, erase or otherwise put this data beyond use.

Retention Period Protocols

All information is retained, stored and destroyed in line with legislative and regulatory guidelines.

For all data and records obtained, used and stored within the Company, we:

• Carry out periodical reviews of the data retained, checking purpose, continued validity, accuracy and requirement to retain

• Establish periodical reviews of data retained

• Establish and verify retention periods for the data, with special consideration given in the below areas:

- the requirements of ALLF
- the type of personal data
- the purpose of processing
- lawful basis for processing
- the categories of data subjects
- Where it is not possible to define a statutory or legal retention period, as per the GDPR requirement, the Company will identify the criteria by which the period can be determined and provide this to the data subject on request and as part of our standard information disclosures and privacy notices (link to privacy notice)
- Have processes in place to ensure that records pending audit, litigation or investigation are not destroyed or altered.

8. Be managed and stored in such a manner that, in the event a data subject submits a valid Subject Access Request seeking a copy of their personal data, this data can be readily retrieved and provided to them.

ALLF has implemented a Subject Access Request procedure by which to manage such requests in an efficient and timely manner, within the timelines stipulated in the legislation.

Data Storage

The IT infrastructure, including e-mails, database and internet access represent a significant investment on behalf of the organisation. ALLF must ensure the systems and access are managed correctly, not abused in how they are used or for what they are used, the parameters and restrictions for their use are defined below.

Data Subject Access Requests
Where a valid, formal request is submitted by a data subject in relation to the personal data held by ALLF which relates to them, such a request gives rise to access rights in favour of the Data Subject.
At its own discretion, ALLF may charge a maximum administrative fee of €6.35 in order to process such requests.
There are specific time-lines within which ALLF must respond to the data subject, depending on the nature and extent of the request. These are outlined in the attached Subject Access Request process document.
ALLF's staff will ensure that such requests are forwarded to the Data Protection Officer in a timely manner, and they are processed as quickly and efficiently as possible, but within not more than 40 calendar days from receipt of the request.

Implementation
As a data controller, ALLF ensures that any entity which processes personal data on its behalf (a data processor) does so in a manner compliant with the Data Protection legislation through a formal Data Processor Agreement.
Regular audit trail monitoring will be done by the Data Protection Officer to ensure compliance with this Agreement by any third-party entity which processes personal data on behalf of ALLF.
Failure of a data processor to manage ALLF's data in a compliant manner will be viewed as a breach of contract, and will be pursued through the courts.
Failure of ALLF's staff or volunteers to process personal data in compliance with this policy may result in disciplinary proceedings.

Procedures

Data Storage

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately. It is ALLF's responsibility to ensure all personal and company data

is nonrecoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

Data access and accuracy

ALLF will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition, ALLF will ensure that:

• It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection

• Everyone processing personal information understands that they are contractually responsible for following good data protection practice

• Everyone processing personal information is appropriately trained to do so

• Everyone processing personal information is appropriately supervised

• Anybody wanting to make enquiries about handling personal information knows what to do

• It deals promptly and courteously with any enquiries about handling personal information

• It describes clearly how it handles personal information

• It will regularly review and audit the ways it holds, manages and uses personal information

• It regularly assesses and evaluates its methods and performance in relation to handling personal information

• All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

The IT infrastructure, including e-mails, database and internet access represent a significant investment on behalf of the organisation. ALLF must ensure the systems and access are managed correctly, not abused in how they are used or for what they are used, the parameters and restrictions for their use are defined below.

Emails and Contents

The primary purpose of the email system is to promote effective communication and this should not be abused.

While email is a fast and efficient method of communication, it must not be overlooked that it has the same legal effect as written communication. Due to the permanent nature of emails and the legal implications to the organisation, employees and volunteers, messages should be written and formatted in the same manner as standard written communications.

The wording, tone and language should be concise and carefully prepared in order to avoid ambiguity, inaccuracy, claims of defamation, breach of confidentiality and the possibility of offending anyone. No form of discriminatory comment, aggression, harassment or bullying is permitted through emails.

All emails sent on behalf of ALLF will have the following disclaimer displayed:

DISCLAIMER

This email and any files attached to it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify A Little Lifetime Foundation, info@alittlelifetime.ie.

Confidentiality

Employees and volunteers are not permitted to register with sites or electronic services in the company/charity name without the prior permission of management. They are not permitted to reveal internal information to any sites, be it confidential or otherwise, or comment on company matters, even if this is during after hours or personal use. Strict confidentiality applies to all electronic communication and data. All personal information or data registered with ALLF in any format, (data base, web forum etc.) will be treated with strict confidentiality at all times.

Monitoring

The organisation retains the right to monitor and record the activities of all users on the system. It retains the right to monitor (intercept and read) each individual's email, Internet and PC activity to ensure the protection of all data, employees and volunteers, and that there is no abuse of privilege.

Abuse and Disciplinary Procedure

Any person found to be abusing the electronic communication system or database will be subject to disciplinary action. This includes any attempt to circumvent system security, including firewalls, put in place to protect the organisation.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection legislation.

In case of any queries or questions in relation to this policy please contact the A Little Lifetime Foundation Data Protection Officer:

Name and contact details of the Data Protection Officer Signed: Mary McGrath

Position: Data Protection Officer

Date: June 1st 2021

Review Date: June 2024