LIFE LTD.

Data Protection Policies and Procedures Manual

TABLE OF CONTENTS

Introduction & Purpose

LIFE Ltd., also known as 'Literacy is for Everyone' ("**LIFE**") needs to collect and use certain information about individuals, such as volunteers of LIFE, and other people LIFE may needs to contact.

This manual explains how LIFE will collect, handle and store such information so as to protect that information, ensure that it is used appropriately and to comply with the law.

Cayman Islands Data Protection Law

The Data Protection Law 2017 (the "DPL") regulates the management of the use of personal data by organisations established in the Cayman Islands as well as organisations established outside the Cayman Islands, that process personal data within the Cayman Islands.

It applies to "personal data" which means any information relating to a living individual who can be directly or indirectly identified.

In order to comply with the law, personal data must be dealt with according to the following eight principles:

1. Lawfulness: be processed fairly and only after meeting specified conditions in the DPL.

2. Purpose limitation: be obtained only for lawful purposes specified in the DPL.

3. Data minimisation: be adequate, relevant and not excessive.

4. Accuracy: be accurate and kept up to date.

5. Retention limitation: not be held for any longer than necessary.

6. Access and rectification: processed in accordance with the rights of data subjects under the DPL.

7. Data security and protection: be protected in appropriate ways to prevent unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Protection for international transfers: not be transferred to a country or territory unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Scope & Responsibilities

For the purposes of the DPL, LIFE will be a "Data Controller" and a "Data Processor".

LIFE will be legally responsible for applying the requirements of the DPL, applying the data protection principles to the personal data that is collected on its behalf, and cooperating with investigations of the Ombudsman.

Notice

LIFE is required to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used; and
- How to exercise their rights.

To fulfil such requirements, LIFE has a Privacy Notice that explains how LIFE collects, uses, discloses, retains, and secures personal data and the legal basis for its actions (Appendix 1). Such Privacy Notice shall be accessible through LIFE's website.

Data Collection

"Personal data" is any information, which, directly or indirectly, relates to an identified or identifiable natural person.

Any type of data can be used to identify an individual. However, whether a data or a set of data actually identifies an individual will depend on the overall context of the processing, which must always be taken into consideration when evaluating whether personal data is being processed.

Personal data can either directly or indirectly identify an individual.

The DPL provides a non-exhaustive list of identifiers, including:

- location data;
- online identifiers (which include IP addresses and cookie identifiers);
- one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the living individual;
- an expression of opinion about the living individual; and
- any indication of the intentions of the data controller or another person in respect of the living individual.

If an individual can be identified directly from the information you are processing, it will constitute personal data.

If an individual can be identified indirectly from the information you have, i.e. by combining it with another source of information, the information you have may constitute personal data. That additional information may be information you already hold, or it may be information that you or a third party can reasonably obtain from another source.

To decide whether data relates to an individual, three elements will need to be considered, either of which can independently trigger data as relating to an individual:

- the **content** of the data, i.e. where the data itself is directly about the individual or their activities;
- the **purpose** of the data being processed, i.e. where the data is intended to be used with regards to an individual, such as to evaluate or influence them; and
- the **results** on the individual of the data being processed, i.e. because the processing outcome will impact their rights and interests.

As such, it is important to consider carefully the overall context of the processing activity in order to decide whether the data relates to an individual.

There are enhanced requirements if the personal data is considered to be "sensitive personal data" which is personal data consisting of:

(a) the racial or ethnic origin of the data subject;

(b) the political opinions of the data subject;

(c) the data subject's religious beliefs or other beliefs of a similar nature;

(d) whether the data subject is a member of a trade union;

(e) genetic data of the data subject;

(f) the data subject's physical or mental health or condition;

(g) medical data;

(h) the data subject's sex life;

(i) the data subject's commission, or alleged commission, of an offence; or

(j) any proceedings for any offence committed, or alleged, to have been committed, by the data subject, the disposal of any such proceedings or any sentence of a court in the Islands or elsewhere.

"Processing" of personal data is defined by the DPL broadly and covers any conceivable use of data which affects it in any way including simply storing or retaining it. It comprises obtaining, recording or holding data, or carrying out any operation or set of operations on personal data, including:

- organising, adapting or altering the personal data;
- retrieving, consulting or using the personal data;
- disclosing the personal data by transmission, dissemination or otherwise making it available; or
- aligning, combining, blocking, erasing or destroying the personal data.

It is only legitimate to process personal data if one of the following conditions is satisfied:

- the individual has given clear **consent** to process their personal data for a specific purpose;
- the processing is necessary for performance of a **contract** with the individual, or because they have asked you to take specific steps before entering into a contract;
- the processing is necessary to **comply with a law** (not including contractual obligations);
- the processing is necessary to **protect the individual's life**;
- the processing is necessary for you to perform a **public function**, or a function of a public nature exercised in the public interest;
- the processing necessary for **legitimate interests** pursued by the data controller or a third party, except where it is unwarranted because of prejudicing the rights and freedoms or legitimate interests of the individual.

The legal basis is recorded in the Privacy Notice.

Data Storage & Security

Personal data may be stored in hard (i.e. paper) copy, or electronically.

For hard copy documents containing personal data the following rules will be applied:

- documents will be kept in locked storage, i.e. a locked filing cabinet or drawer;
- documents will not be left where unauthorised people can see them; and
- documents will be shredded or disposed of securely when no longer required.

For electronic documents they must be protected from unauthorised access or accidental deletion and the following rules will be applied:

- Data should be **protected by strong passwords** that are changed regularly and never shared;
- Data will **not be stored on removable media** (like a CD or DVD);
- Data should only be stored on **designated drives and servers**, and should only be uploaded to a **recognised cloud computing service**;
- Servers containing personal data should be **sited in a secure location**, away from general office space;
- Data stored outside the recognised **cloud computing service** should be **backed up frequently** and such backups should be **tested regularly**;

- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones; and
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data Use & Transfer

Personal data shall only be used for the purpose for which it was obtained by LIFE.

Personal data will not be transferred outside of the Cayman Islands unless the destination is the European Union or a country considered adequate by the European Commission pursuant to Article 54(3) of the EU General Data Protection Regulation (EU 2016/679) unless one of the following exceptions is applicable:

- made with the individual's consent;
- necessary for the performance of a contract between the individual and the organisation, or for pre-contractual steps taken at the individual's request;
- necessary for the performance of a contract made in the interests of the individual between the controller and another person;
- necessary for important reasons of substantial public interest;
- necessary for the establishment, exercise or defence of legal claims;
- necessary to protect the vital interests of the data subject;
- made in regard to public data on a public register, and any conditions subject to which the register is open to inspection are complied with;
- made on terms of a kind approved by the Ombudsman as ensuring adequate safeguards for the individual(s);
- authorised by the Ombudsman as ensuring adequate safeguards for the individual(s); or
- required under international cooperation arrangements between intelligence agencies or regulatory agencies, if permitted or require under an enactment or an order issued by the Grand Court.

Data Accuracy

LIFE is required to take reasonable steps to ensure that personal data that has been collected remains accurate and up to date.

Access Requests

All individuals who are the subject of personal data held by LIFE are entitled to access their own personal data - a “Subject Access Request”.

In addition, LIFE is required to provide the following information:

- the purposes of your processing;
- the categories of personal data concerned;
- the recipients or classes of recipient you disclose, or may disclose, the personal data to;
- any countries or territories outside the Cayman Islands to which you do, or intend to, transfer the personal data;
- the general measures you take to ensure the security of the personal data;
- any information available as to the source of the personal data;
- the reasons for any automated decision made in relation to the individual, including the individual’s performance at work, creditworthiness, reliability or conduct; and
- the right to make a complaint to the Ombudsman.

There is a 30-day time-limit for complying with a request and no charge may be made.

If a request is made by a law enforcement agency LIFE will obtain legal advice before complying with such request.

Data Retention Policies

Subject to the DPL, personal data will be retained in a manner consistent with the DPL and no longer than is necessary for the purposes for which it has been collected.

(a) The DPL does not dictate how long LIFE should keep personal data. Therefore, it is up to LIFE to consider and justify its policy on retention periods. LIFE should consider the following when determining how long it should keep the information:

(b) the purpose for which the data was obtained;

(c) if would be required to confirm that the relationship existed;

(d) if retention is required to defend possible future legal claims;

(e) if retention is required to comply with legal or regulatory requirements;

if retention is required to comply relevant industry standards or guidelines.

LIFE reviews the data it holds and deletes or anonymises anything it no longer needs. LIFE has established a system for ensuring that it keeps to its retention periods in practice, and for reviewing its retention policy and the data it is holding at regular intervals. The policy allows early deletion of information in certain circumstances when individuals withdraw their consent or LIFE ceases controlling or processing their data.

LIFE reviews its retention at the end of any standard retention period and at regular intervals before the end of standard retention period. If the information is determined as no longer needed, LIFE can either delete it or anonymise it.

Data Subjects Rights

Subject to the DPL, data subjects have the following rights regarding their own personal data:

- The right to be informed: individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the DPL.
- The right of access: individuals have the right to access their own personal data.
- The right to rectification: the DPL includes, indirectly, a right for individuals to have inaccurate personal data rectified or completed if it is incomplete, insofar as the data controller is convinced of the validity of the request.
- The right to stop/restrict processing: individuals have the right to require that processing stop, or not begin, or cease processing for a specified purpose or in a specified way.
- The right to stop direct marketing: the DPL gives individuals an absolute right to stop the processing of their personal data for direct marketing purposes.
- The rights in relation to automated decision making: the DPL has provisions on solely automated individual decision-making (making a decision exclusively by automated means without any human involvement).
- The right to seek compensation: an individual suffers damage due to a contravention of the DPL by a data controller may seek compensation in the courts.
- The right to complain: an individual has the right to complain to the Ombudsman about any perceived violation of the DPL.

The above rights are not absolute and may be restricted in certain specified circumstances. Exemptions may also apply; whereby specified rights or other provisions of the DPL do not apply.

Contracts Between Data Controller and Data Processor

Not applicable.

Data Breach

The DPL introduces a duty on all data controllers to report personal data breaches to the Ombudsman and the individual(s) whose data was breached, unless the breach is unlikely to prejudice their rights and freedoms.

The DPL defines a “personal data breach” as: “personal data breach” means 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. It can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

Data controllers shall report a personal data breach to the Ombudsman and the individual(s) concerned without undue delay, but not longer than five days after they should, with the exercise of reasonable diligence, have been aware of the breach, describing:

- the nature of the breach;
- the consequences of the breach;
- the measures proposed or taken by the data controller to address the breach; and
- the measures recommended by the data controller to the data subject of the personal data in question to mitigate the possible adverse effects of the breach.

All data breaches must be reported unless the breach is unlikely to prejudice the rights and freedoms of the affected data subjects. A data controller who contravenes the above commits an offence and is liable on conviction to a fine of one hundred thousand dollars.

Contact Person

The Ombudsman:

When data controllers want to report a personal data breach to the Ombudsman or when data subjects consider that their personal data has not been handled correctly, or they are not satisfied with data controller’s responses to any requests they have made regarding the use of their personal data, and want to complain to the Cayman Islands’ Ombudsman.

The Ombudsman can be contacted by calling: 1-345-946-6283 or by email at info@ombudsman.ky. For more contact details, please refer to the contact page on the website: http://ombudsman.ky/get-in-touch.

LIFE:

For further information on the collection, use, disclosure, transfer or processing of personal data or exercise by LIFE or the rights of data subjects, please contact info@life.org.ky.

Appendix 1

Privacy Notice

Scope

This privacy notice explains how LIFE collects, uses, discloses, retains and secures personal data. The policy explains the legal basis for the processing of personal data and also lists the individual data subject rights under the Cayman Islands' Data Protection Law, 2017 (the "**DPL**"), which came into effect on 30 September 2019.

Overview

LIFE is a data controller and data processor in respect of your personal data for the purposes of the DPL and as such is responsible for ensuring that it uses your personal data in compliance with the same.

The key principles LIFE applies when processing personal data are as follows:

- Lawfulness: LIFE will only collect personal data in a fair, lawful and transparent manner;
- Purpose limitation: LIFE will only collect personal data for specified, explicit and legitimate purposes;
- Data minimisation: LIFE will limit the collection of personal data to what is directly relevant and necessary;
- Accuracy: LIFE will try and keep personal data accurate and up to date while there continues to be a relationship, and in certain circumstances after that relationship has ended;
- Retention limitation: LIFE will retain personal data in a manner consistent with the DPL and no longer than is necessary for the purposes for which it has been collected. This is expected to be no longer than 10 years, but is determined by the residency of the person on whom data is held;
- Access and rectification: LIFE will process personal data in accordance with a data subject's legal rights under the DPL;
- Data security and protection: LIFE will implement technical and organisational measures to ensure an appropriate level of data security and protection. Such measures provide for the prevention of any unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to that data; and
- Protection for international transfers: LIFE will ensure that if personal data is transferred outside the Cayman Islands, it is adequately protected or the transfer is otherwise permissible under applicable law.

Personal data that LIFE might use

LIFE (or any of its affiliates, agents, employees, delegates or sub-contractors) might process the following personal data:

Information provided to LIFE by you. This might include your name and address (including proof of the same), contact details, date of birth, gender, nationality, photograph, signature, copies of identity documents, occupational history, job title, and residency. Such information might be provided in an application form, face to face, by telephone, by email or otherwise; and

(a) Information that LIFE obtains from other sources including for the purposes of "know-your-client" procedures, information from government or public bodies, public websites and other public sources, the applicant's advisers or from intermediaries.

(b)

Uses of your personal data

Your personal data may be stored and processed by LIFE for the following purposes:

Compliance with legal and regulatory obligations and industry standards;

(a) Assessing and processing applications for volunteers for LIFE; and

(b)

To protect LIFE's legal rights and interests.

(c)

Legal Basis for processing personal data

The DPL sets out a number of different circumstances in which there is an entitlement to process personal data including but not limited to consent, contractual obligation, legal compliance and legitimate interest.

Disclosure of personal data

LIFE may, in accordance with the purposes set out herein, disclose your personal data to third parties including, schools and governmental authorities.

International transfer of personal data

LIFE may disclose personal data to competent authorities, courts and bodies as required by applicable law or as requested by such entities, or to affiliates for internal investigations and reports.

Retention of personal data

The retention period for the holding of personal data will vary and will be determined by criteria including the purposes for its use and retention periods prescribed by law and other legal obligations.

Security of personal data

LIFE employs appropriate technical and organisational measures to protect against unauthorised processing, accidental loss or destruction of, or damage to, personal data.

Data Breach

LIFE, and those processing personal data on LIFE's behalf, must have effective measures in place to enable the detection, investigation, and (where appropriate) timely reporting by LIFE to the Ombudsman (and impacted individuals) of personal data breaches. If there is a personal data breach, LIFE will, without undue delay and, in any event, not later than five days after having become aware, notify the personal data breach to the Ombudsman and the impacted individuals. LIFE will also specify in such notice the measures taken in light of the breach, and those which individuals are recommended to take. LIFE will only refrain from reporting where the personal data breach is unlikely to prejudice the rights and freedoms of affected individuals. All data breaches will be recorded and investigated in order to prevent any reoccurrence.

What rights do individuals have in respect of personal data?

Individuals have a right to be informed how personal data is processed and this privacy notice fulfils LIFE's obligation in this respect.

Individuals have a right to request access to their personal data, the right to request rectification or correction of personal data, the right to request that processing of personal data be stopped or restricted and the right to require that LIFE cease processing personal data for direct marketing purposes.

If you consider that your personal data has not been handled correctly, or you are not satisfied with LIFE's responses to any requests you have made regarding the use of your personal data, you have the right to complain to the Cayman Islands' Ombudsman. The Ombudsman can be contacted by calling: 1-345-946-6283 or by email at info@ombudsman.ky.

Contacting LIFE

For further information on the collection, use, disclosure, transfer or processing of your personal data or the exercise of any of the rights listed above, please contact **LIFE** at +1 345 815 8525 or info@life.org.ky