Lewisham Islamic Centre

General Data Protection Regulation (GDPR) Policy

Version: 1.0

Policy owner: Lewisham Islamic Centre

Date of approval: 21/04/2018

Effective from: 25/05/2018

Next review: 01/01/2022

Revision history

Version	Date	Description of Revision	Version	Date	Description of Revision
1.0	21/04/18	Policy finalized			
2.0	25/12/19	CCTV added			
3.0	01/01/21	Amended Charity number			

The latest version of this policy will always be on the intranet.

Lewisham
ISLAMIC·CENTRE

Table of Contents

1. DEFINITIONS

This document uses definitions applicable to **General Data Protection Regulation (GDPR), 2018.**

I. **"Biometric Data"** Any personal data relating to the physical, physiological, or behavioural characteristics of an individual which allows their unique identification.

II. **"Consent"** Freely given, specific, informed and explicit statement or action signifying agreement to the processing of personal data.

III. **"Controller"** The **"controller"** for the **purposes** of this policy is **LIC**. **The controller** is the natural or legal person who either alone or jointly with others determines the purposes and means of processing of personal data. Or **"Data Controller"** The entity that determines the **purposes**, **conditions** and means of the **processing** of **personal data**.

IV. **"Data Subject"** The **"data subject"** is any natural person about whom information is obtained, stored and/or processed by **LIC** or any person or **departments** under the proprietorship of **LIC**. **"Data Subjects"** Include service-users, employees, volunteers, donors, students, governors, trustees, contractors of **LIC** and any other person whose personal data is collected and processed by or on behalf of **LIC** for any reason. **For example, PayPal & JustGiving**

V. **"Data Erasure"** Also known as the **Right to be Forgotten**; it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data.

VI. **"Data Portability"** The requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with **another controller.**

VII. **"Data Processor"** The entity that processes data on behalf of the Data Controller.

VIII. **"Data Protection Officer"** 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.

IX. **"Directive" –** a legislative act that sets out a goal that all EU countries must achieve through their own national laws **e.g. Data Protection Act, 1998.**

X. **"Encrypted Data"** Personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access

XI. **"Filing System"** Any specific set of personal data that is accessible according to specific criteria, or able to be queried

XII. **"Natural Person"** A living person; A human being; The term "**natural person**" does not include any **"legal entity"** such as a company, partnership or corporation.

XIII. **"Personal Data"** Article 4 of the GDPR legislation defines personal data **as "any information relating to an identified** or **identifiable natural person** or **Data Subject… who can be identified, directly or indirectly, by reference to an identifier."** The word **"identify" in the definition** can be anything from a **name**, **location data, a photo**, **an email address**, **bank details, posts on social networking websites, medical information, cookies** or **online identifiers such computer IP addresses. Other data, such as economic, cultural and mental health information,** are also considered **personally identifiable information.**

- **GDPR** not only applies to **automated personal data but also manual filing systems where personal data are accessible according to specific criteria.** This could include chronologically ordered sets of manual records containing personal data. Personal data that has been **pseudonymised** – e.g. key-coded – can fall within the scope of the **GDPR rules** depending on how **easy or hard** it is to attribute the **pseudonym** to a particular individual. **Thus, any data that could identify an individual need to be considered.**

- **Anything that counted as personal data under the Data Protection Act,1998 also qualifies as personal data under the GDPR.**

XIV. **"Personal Data Breach"** A breach of security leading to the accidental or unlawful access to, destruction, misuse, etc. of personal data.

XV. **"Processor"** A "processor" is a natural or legal person who processes personal data under the direct and express instructions of a **controller**.

Lewisham
ISLAMIC·CENTRE

XVI. **"Processing"** Any operation which is performed on personal data such as but not limited to collection, recording, organisation, structuring, storage, alteration, retrieval, disclosure by transmission, dissemination, restriction, erasure or destruction of personal data.

XVII. **"Privacy by Design"** A principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition.

XVIII. **"Data Protection Impact Assessments" (DPIAs)** (previously known as **Privacy Impact Assessments or PIAs under the Data Protection Act, 1998**) **An assessment on the impact of the envisaged processing operations on the protection of personal data;** mandated by the **GDPR.** It is 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; thus, complying with data protection obligations and meeting individuals' expectations of privacy.

XIX. **"Processing" Any** operation performed on **personal data, whether or not by automated means, including collection, use, recording, etc.**

XX. **"Profiling"** Any automated processing of personal data intended **to evaluate, analyse, or predict data subject behaviour.**

XXI. **"Pseudonymisation"** The processing of personal data such that it can **no longer be attributed to a single data subject without the use of additional data.** Additional data stays separate to ensure non-attribution.

XXII. **"Recipient"** Entity to which the personal data are disclosed

XXIII. **"Regulation"** A **binding legislative act** that **must** be **applied** in its **entirety** across the EU. It is important to note that the **GDPR** is a regulation; in contrast, the previous legislation **(Data Protection Act. 1998),** was a **directive**.

XXIV. **"Right to Access"** Also known as **Subject Access Right**; it entitles the data subject to have access to information about their personal data that a controller has concerning them.

XXV. **"Special Category Data"** Certain data that is sensitive in nature. **Special category** reveals **racial** or **ethnic origin**, **political opinions, religious or philosophical beliefs, trade-union memberships of any natural person.** Any other data such as **genetic** or **biometric data** which can uniquely identify a natural person or data concerning the sex life or sexual **orientation of a natural person is also special category data.**

1. PURPOSE OF THIS POLICY

1.1 The purpose of this **GDPR policy** is to communicate to **staff** and **volunteers** of departments under the proprietorship of **Lewisham Islamic Centre (LIC)** and to **donors**, **supporters** and **service-users** of **LIC** the approach that **LIC** intends to take when handling the personal data of any natural person.

1.2 A key focus of this **GDPR policy** is to ensure that the **privacy rights** of individuals are **protected** and **strengthened**; **empowering individuals** to have more control over their **personal data**.

1.3 This also entails **a right to be forgotten** when individuals **no longer** want their data to be processed by **LIC**, **provided that there are no legitimate grounds for retaining them**.

1.4 **All staff** involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to the **GDPR principles.**

1.5 This document applies to the operation of **LIC** in England and Wales.

1.6 **LIC** shall comply with data protection law. **The law prior to 25.05.18 is derived from the Data Protection Act, 1998** and **from 25.05.18** will be derived from the **General Data Protection Regulation (GDPR**) which came into force on **25.05.16** and becomes applicable on **25.05.18**.

1.7 Compliance with this **policy** will be the responsibility of the **LIC Data Protection Officer**.

1.8 Every person who is **employed** or **volunteers** for **LIC** is required to **adhere** to this policy to the best of their ability. If there are any concerns regarding the application of this policy, it is the responsibility of the person with the concern to contact **LIC's** data protection manager at the first opportunity either directly or in writing.

2. OUR COMMITMENT

2.1 LIC is **committed** to, the **protection** of all **personal** and **sensitive** data for which it holds; **its responsibility as the Data Controller** and **the handling of such data in line** with the **GDPR**.

2.2 All data within **LIC's** control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates. The definitions of personal and sensitive data shall be as those published by the ICO for guidance: **https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/**

2.3 Changes to data protection legislation shall be **monitored** and **implemented** in order to **remain compliant** with **all requirements**.

2.4 LIC is also committed to ensuring that all staff or volunteers and **all the departments that handle personal data** and provide services at **LIC** are aware of **GDPR** policy and its legal requirements and that, adequate training is provided. **This will bolster;**

- **LIC** do its utmost best to get this right by not only meeting its donor's legal requirements, but also giving each one of them a great experience of supporting **LIC**.

- **LIC** to reciprocate these legal requirements and great experience whilst managing staff, volunteers, contractors and service-users' personal data.

- **LIC** to adopt a whole organisation approach, with a strategy agreed at trustee level. Since Volunteers are no different to employees, they will also be trained and equipped to protect data.

2.5 **LIC** will arrange an **audit** of what personal data we hold, where it came from and whom we share it with to get a sense of what we'll need to do next.

2.6 Consent will be reviewed by explaining clearly without ambiguity through a statement or clear affirmative action such as; actively ticking a box in our **Privacy Notice** why **LIC** is collecting personal data and how **LIC** intends to use it. The **rights** of the individual will always take precedence over **LIC's** legitimate interest of furthering its cause. **For instance**,

- The **"right to be forgotten"** where people can request the removal of personal data, either if they no longer want **LIC** to have it or if it is no longer used for the purpose it was collected will be exercised.

- Data will be kept **up to date** and accurate and not for longer than is necessary.

- To give people clear information, our **Privacy notice** will also include the following sections: - **"Find out what information we hold on you"** and **"Remove all information about me".**

- **LIC** will ensure that right procedures are in place to **detect, report** and **investigate a personal data breach.** We will also review information from the ICO regularly to keep on top of developments in this area.

- Finally, **LIC** will **review its current method of processing data whilst ensuring that plans are in place to make any changes that we need before the 25th of May 2018.**

3. NOTIFICATION

3.1 **LIC** data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

3.2 Changes to the type of data processing activities being undertaken shall be notified to the ICO by **LIC** and details amended in the register.

3.3 Breaches of personal or sensitive data shall be notified immediately by **LIC** to the individual(s) concerned and the ICO.

4. GDPR SCOPE

4.1 The GDPR came into force on the **25th of May 2016** and would become applicable by law on the **25th of May 2018**; even post-Brexit. (UK's commitment to leaving the EU has no impact on this date or the regulation)

4.2 However, it is also important to remember that the **GDPR** is **merely an extension of previous data protection laws and not a complete overhaul (as many are thinking). The aim** of the law is not to restrict, but to **merely clarify previously ambiguous regulations and ensure consumer rights are protected.**

4.3 Because **GDPR** is a regulation, not a directive, the UK does not need to draw up new legislation instead, it will apply automatically. Any data that an Organisation holds that is not **GDPR compliant** by this date would have to be **deleted/erased regardless of what form it's kept in**. (Documents in filing cabinets, records and databases of students, staff, volunteers or donors, monitoring what's happening day-to-day on the premises through CCTV etc all need to be GDPR compliant)

4.4 The drivers of GDPR are twofold.

- **First**, the EU wants to give people more control over how their personal data is used, bearing in mind that many companies such as **Facebook** and **Google swap access** to people's data for use of their services. The outgoing legislation was enacted before the internet and cloud technology created new ways of exploiting data, and the **GDPR** seeks to address that. **By strengthening data-protection legislation and introducing tougher enforcement measures, the EU hopes to improve trust in the emerging digital economy.**

- **Second**, the EU wants to give businesses a simpler, clearer legal environment in which to operate, **making data-protection law identical throughout the single market** (the EU estimates this will save businesses a collective €2.3 billion a year).

4.5 **GDPR** adds extra responsibilities to the **Data Protection Act 1998 thereby replacing it. It** aims at; **eliminating any ambiguity around consent** thus**, limiting the number of individuals giving their consent without realising.**

4.6 **GDPR** has been designed to ensure that all **personal data** is handled and managed in a way that gives **individuals** the **right** to **choose** how their **data** is **collected, stored** and **processed; thereby impacting on how organisations handle data. It** takes into account the massive changes in technology since **the Data Protection Act was introduced in 1984.**

4.7 An **individual** will have the right to have their data **permanently deleted/erased**. **Parental consent** will be required for minors (under 16 years old) and accountability for non-compliance is fully explicit.

4.8 **Subject access requests (SARs)** are free of charge and must be done within 30 days. Individuals **must opt-in** whenever data is collected and there must be **clear privacy notices**. These notices must be concise and transparent; and **consent** must be able to be withdrawn at any time. **The need for consent underpins GDPR because:-**

- **Consent** must be an **active, affirmative action by the data subject, rather than the passive acceptance under some current models that allow for pre-ticked boxes or opt-outs.** Under **the GDPR**, **"consent"** of the data subject means *'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'* (Article 4(11)).

- **The key issue here is that consent would require a 'clear affirmative action' with the ability to be withdrawn later.** Controllers must, **keep a record of how and when an individual gave consent** and enable an individual to withdraw their consent whenever they wish to do so.

- **If an organisation's current model for obtaining consent doesn't meet these new rules, they'll have to bring it up to scratch or stop collecting data under that model when the GDPR applies on the 25th of May 2018.**

- **Controllers** must now store people's information in commonly used formats **(such as CSV files) so that they can move a person's data to another organisation (free of charge) if the person requests it. Controllers must do this within one month.**

4.9 The **GDPR** applies to personal data held by an organisation relating to EU residents regardless of where it is processed and other residents or travellers living in the **GDPR jurisdictions;** forcing organisations worldwide to comply with its requirements. **Essentially: -**

- The **GDPR** applies to **'Controllers'** of data who comprise **profit seeking organisations, non-profit** organisations/**charities** or government bodies). **Regardless the size of their company, Controllers have the legal obligation to state how and why personal data is processed.**

- This **regulation** enforces **a duty of care** and **best practice** towards all organisations that handle personal data.

- Apart from **LIC**, **OTS** and **YMA** also handle a large amount of personal data. **Since they handle what the GDPR refers to as special category data, they are subject to tighter controls.**

- With such **a major emphasis of evidencing compliance,** it's important that **all departments under the proprietorship of LIC** demonstrate that they are **all on board**; when it comes to **data protection**.

- **Part of the process of becoming compliant is to ensure that each and every one of us has received adequate training relevant to their day to day activities** at **LIC** and that, everyone understands both the **cyber security implications of their actions** and the **guidelines about the protection of personal data.**

- **With the increased emphasis on accountability**, **more pressure will be on departmental heads to ensure their staff receive the necessary training**. Please note that the **GDPR will also impact anyone who handles personal data, even if it's just an attendance register.**

5. GDPR PRINCIPLES

5.1 Every person working in **Lewisham Islamic Centre (LIC)** must adhere to the following **6 GDPR** principles when dealing with personal data.

a) Lawfulness, fairness and transparency

Data must be processed lawfully, fairly and in a **transparent/unambiguous** manner in relation to individuals/subjects; **Transparency**: Tell the subject what data processing will be done. **Fairness**: What is processed must match up with how it has been described. **LIC privacy notice shall include our lawful basis for processing as well as the purposes of the processing.**

Lewisham ISLAMIC·CENTRE

NOTE:- Once the GDPR is in effect, it will be much harder to swap between lawful bases if the original basis is deemed invalid. **This will inevitably result in breach of the GDPR as the lawful basis was not clearly identified from the start.**

b) Purpose limitations

Personal data can only be collected for **specified**, **explicit** and **legitimate purposes** and not further processed in a manner that is **incompatible** with those purposes ('purpose limitation'). In other words, data can only be used **for a specific processing purpose that the subject has been made aware of and not further in a manner that is incompatible with those purposes without consent.**

c) Data minimisation

Data collected on a subject should be "**adequate**, **relevant** and **limited** to what is necessary in relation to the purposes for which they are processed" [article 5, clause 1(c**)]. In other words, no more than the minimum amount of data should be kept for specific processing.**

d) Accuracy

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.** Data holders/**controllers** should build rectification processes into data management / archiving activities for subject data. **Baselining should be adopted to ensure good protection against identity theft. Yearly data cleansing exercise should be adopted.**

e) Storage limitation

Regulators expects personal data is kept in a form which permits identification of data subjects **for no longer than is necessary for the purposes for which personal data are processed ('storage limitation')**. In summary, **data no longer required should be removed**. **For example, if someone applied for a job and did not secure a position, their data can only be kept on record for a maximum period of 1 year only after which it should be destroyed. A**

donor's data via a merchant service or direct debit that has been stopped by the individual should also be kept for 1 year only thereafter it should be deleted/destroyed.

f) Integrity and confidentiality

Processed in a manner that ensures **appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures ('integrity and confidentiality'). USB** that has personal data must be **encrypted**.

6. EIGHT DATA SUBJECT RIGHTS

6.1 All 8 data subject rights are, in effect, LIC's obligation. **LIC** is aware that is incumbent upon it **as a Controller** to facilitate the exercise of these rights.

6.2 Every data subject has the following rights which **LIC** shall uphold in a timely manner in order to comply with the **GDPR**: To **comply** with the **GDPR, LIC** shall have procedures in place for each of them.

I. **Right to be informed** - To ensure that personal data is processed fairly, **LIC** shall provide **certain minimum information to data subjects, regarding the collection and further processing of their personal data**. As stated by the **GDPR**, such information provided shall be in a **concise, transparent, intelligible and easily accessible form, with clear and plain language**. Exemptions may apply, and **LIC** may restrict the provision of information where it is necessary and proportionate.

II. **Right of access** - Data subjects have **the right to file a subject access requests (SARs**) and **obtain** from **LIC** a **copy of their personal data, together with an explanation of the categories of data being processed and the purposes of such processing.** In conformity with the **GDPR**, **LIC** shall respond to **SARs** within **one month** with information, including details of the period for which the data will be stored (or the criteria used to determine that period) and information about other rights of data subjects. Individuals have the right to be aware of and verify the lawfulness of the processing **LIC** is carrying out.

❖ The data subject shall have the right to obtain from **LIC** confirmation as to whether personal data concerning him or her are being processed, **and, where that is the case, access to the personal data and the following information:**

1. The purposes of the processing;

2. The categories of personal data concerned;

3. Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

4. The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

5. The right to lodge a complaint with a supervisory authority;

6. Where the personal data are not collected from the data subject, any available information as to their source;

7. The right to obtain a copy shall not adversely affect the rights and freedoms of others.

NOTE

✓ There is no requirement for a request to be in writing. Therefore, it is good practice to have a policy for recording details of all the requests you receive, including verbal requests.

✓ **LIC shall** provide a copy of the information free of charge.

✓ **LIC** shall provide the information requested in a commonly used electronic form without delay and at the latest within one month of receipt.

III. Right of rectification –Data subjects have the right to require **LIC** to **correct / rectify errors** in personal data held. They shall have the right to obtain from **LIC without undue**

delay the rectification of inaccurate personal data concerning them. Considering the purposes of the processing, the data subject shall have **the right to have incomplete personal data completed, including by means of providing a supplementary statement.** In addition, **LIC must also rectify inaccurate personal data when it becomes apparent.,**

- ✓ An individual can make a request for rectification **verbally** or in **writing**. Therefore, it is **good practice** to have a **policy** for **recording** details of the **requests** you receive, including those made by **telephone** or **in person**.

- ✓ Check with the requester that you have understood their request as this can help avoid later disputes.

- ✓ Maintaining a log of verbal requests is highly recommended.

- ✓ Request for more supplementary information if there are reasonable doubts of an individual's identity. Requests for verification should be **reasonable** and **proportionate**, taking into consideration the nature of the personal data **LIC** holds and its relationship with the individual.

- ✓ **If you refuse a request for rectification, you must tell the individual, informing them of their right to raise a complaint with the Information Commissioner or taking matters to court.**

- ✓ If requests are manifestly unfounded or excessive, because they are repetitive and **LIC** is able to demonstrate that the request is manifestly unfounded or excessive, **LIC** can:

    - **charge a reasonable fee considering the administrative costs of providing the information;**
      or
    - **refuse to respond.**

- ✓ **In addition, a record of the decisions and reasoning made must be documented as it may be required by the Information Commissioner.**

IV. **Right to erasure – The right to erasure is also known as the "the right to be forgotten". This means that if LIC receives such a request, LIC shall ensure that the data is deleted without undue delay.** Data subjects can request **LIC** to delete their personal data when the data is no longer needed for its original purpose, or where the processing is based on the consent and **the data subject withdraws that consent (and no other lawful basis for the processing exists).** The broad principle **underpinning** this right is to **enable** an individual to **request the deletion or removal of personal data where there is no compelling reason for its continued processing.**

What does **LIC** need to consider when deciding if the right to erasure applies? First and foremost, the GDPR does not specify how to make a request, so an individual can do so verbally or in writing.

LIC shall put into place a policy for recording details of the requests it receives, particularly those made by telephone or in person (verbal requests). LIC shall also seek clarity before recording requests to later disputes.

LIC shall erase personal data without undue delay if:

- The processing of the personal data will infringe **the GDPR protection principles**;
- **LIC** does not meet safeguards for **archiving** and processing of **sensitive personal data**; or
- **LIC** has a **legal obligation** to erase the data.

If deletion is not technically possible, **LIC** shall at least take **reasonable steps** to put the personal data **'beyond use'**

V. **Right to restriction** – This is a **new** feature of the **GDPR**. It defines the restriction of processing as the 'marking of stored personal data with the aim of limiting its processing for the future'. In certain circumstances when **personal data** either **cannot** be **deleted** because the data is required for the purposes of exercising or defending legal claims or where the data subject does not wish to have the data deleted, **LIC** may continue to store the data but not further process them; whilst limiting their access using passwords and other access controls.

Examples of personal data in this category and cannot be deleted are **Marriage, Divorce and Khula certificates.**

- ✓ Any restriction **LIC** applies needs to be justified as necessary and proportionate. In deciding on proportionality **LIC** shall balance the rights of the data subject against the harm disclosure would cause. **LIC shall only** limit the information it provides only to the extent that it would prejudice the purposes stated above.
- ✓ There is also an obligation for **LIC** to inform the data subject when this limitation is in place, explaining its existence and the reasons unless providing this information itself undermines the purpose of imposing the restriction. **LIC shall k**eep a record of its decisions and provide this reasoning to the Information Commissioner if required.

VI. **Right to portability** – This is a new feature of **GDPR**. This permits the data subject to receive a copy of his or her personal data in a commonly used electronic format or a portable machine-readable form from **LIC,** and to have it transferred to another controller if so desired without hindrance from **LIC;** where technically feasible. **LIC** shall be obliged to exercise this right only if it does not adversely affect the rights and freedoms of others.

VII. **Right to objection** – Data subjects have a right to object to processing of their personal data on certain grounds, in addition to the right to object to processing carried out for the purposes of profiling or direct marketing. **LIC** shall no longer process the personal data unless **LIC is able to** demonstrate **compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for, the establishment, exercise or defence of legal claims.**

VIII. **Rights in relation to automated decision making and profiling.** Data subjects have the right not to be subject to decisions based **solely on automated processing which significantly affect them.** Rights in relation to automated decision making and profiling is where any computerised system could decide based on data and a set of automated rules. **Individuals have the right to insist on human intervention to express their point of view and or obtain an explanation of the decision and the ability to challenge it.**

6.3 Any employee or volunteer of LIC who receives or becomes aware of any request from a data subject must forward **that request to the data processing manager immediately**.

6.4 Data subjects **seeking** to **exercise** any of the **8 data subject rights** are requested to make their request to the **data processing manager at LIC to ensure a prompt and effective response.**

7. CONTROLLER's/LIC's OBLIGATIONS (ACCOUNTABILITY AND GOOD GOVERNANCE)

7.1 In addition to the **data subject rights**, which themselves amount to **LIC's** obligations, **LIC** shall comply with other obligations when processing the personal data of natural persons.

7.2 **LIC** shall put into place comprehensive but proportionate good governance measures. Good practice tools that the ICO has championed for a long time such as **Data Protection Impact Assessment (DPIAs)** formerly known as **privacy impact assessments (PIAs)** and **privacy by design** will **be adopted to avert and minimise the risk of breaches and uphold the protection of personal data.**

7.3 Practically, this is likely to mean that **LIC** shall adopt more policies and procedures although many will already have good governance measures in place.

7.4 **LIC** shall demonstrate compliance by implementing appropriate technical and organisational measures that include **internal data protection policies** such as **staff training, internal audits of processing activities, and reviews of internal HR policies**. In addition, **LIC** shall:

- maintain relevant documentation on its processing activities;
- where appropriate, appoint a data protection officer; and

- implement measures that meet the principles of data protection by design and data protection by default.

7.5 Such measures shall include among many others: **data minimisation; pseudonymisation; transparency, where appropriate; creating and improving security features on an ongoing basis;** or **DPIAs** where appropriate.

I. DATA MINIMISATION

LIC shall only collect personal data as is required to do the required processing. This shall differ depending upon whether the data subject is an employee, a volunteer or donor or service-user.

II. DATA RETENTION

- **LIC** shall only retain personal data for as long as is **reasonably required by law or best practice** following the last contact with the data subject. The retention period shall differ depending upon whether the data subject is an employee, a volunteer or donor or service-user.

- **LIC** shall have a policy of carrying out **data cleansing exercise annually** and as a result, data will be retained for no longer than **one year in excess of the required retention period**.

III. PRIVACY BY DESIGN

- **LIC** shall have the responsibility of designing and engineering its systems so that personal data is not misused, and that it is stored and processed in a manner which is; consistent with minimising the opportunity for data loss and unlawful basis.

IV. RECORD KEEPING.

LIC as controller shall have the responsibility to keep written records (which may be stored in electronic form) in accordance with Article 30. These records are (as applicable to **LIC**):

A. Name, contact details of **LIC** as controller;

B. The purposes of the processing;

C. Description of the categories of data subjects and of the categories of personal data;

D and E are not applicable at LIC)

D. Categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

E. Where applicable, transfers of personal data to a third country (outside of the EEA) or an international organisation, including the identification of that third country or international organisation and, in the case of transfers carried out in relation to performance of a contract between **the controller** and the data subject, a description of suitable safeguards in place to protect the rights and freedoms of the data subject;

F. Where possible the envisaged time limits for retention of the different categories of data;

G. **A general description of the technical and organisational security measures in place to safeguard the rights and freedoms of the data subject.** These records may be made available to the regulator/**ICO** on request.

V. INFORMATION SECURITY MEASURES

LIC has put in place and will continue to monitor and maintain its systems, processes and procedures to ensure and assure that the personal data of **data subjects**, be they **employees**, **volunteers**, **donors**, **contractors and service-users**, are kept securely and safely at all times.

These measures include but are not limited to: **encryption of all data sets at rest, control of all backup datasets which are in any event encrypted; and maintaining physical and logical security in relation to access to any personal data.**

The person responsible for information security at **LIC** is_____, the Information Technology Manager.

VI. DATA PROTECTION BREACHES

- **LIC** shall ensure that all staff understand **what constitutes a data breach**, as it is more than a loss of personal data.

- **LIC** shall ensure that an **internal breach reporting procedure is in place as it will help decision-making about whether we need to notify the Information Commissioner or the public.**

- Any employee of **LIC** or any volunteer working with **LIC** who becomes aware of a data protection breach or a possible data protection breach is required to inform the data protection manager as soon as possible.

- **LIC** shall ensure that **robust breach detection, investigation and internal reporting procedures are in place.**

NOTE

If unaddressed, data breach is likely to have a significant detrimental effect on individuals. For example, it will result to:

- Discrimination;
- Damage to reputation;
- Financial loss;
- Loss of confidentiality or any other significant economic or social advantages.

- On becoming aware of a breach, **LIC** as controller shall be obliged to inform the **ICO** within **72 hours. LIC shall also inform d**ata subjects of any breach affecting their personal data without undue delay unless **LIC** is able to demonstrate that the data breach is unlikely to result in a risk to the rights and freedoms of the data subjects. **LIC** shall include:

  - ❖ The nature of the personal data breach

  - ❖ The name and contact details of the data protection officer (if relevant) or other contact point where more information can be obtained;

  - ❖ A description of the likely consequences of the personal data breach; and

  - ❖ The categories and approximate number of personal data records concerned;

❖ A description of the measures **LIC** has taken, or propose to take, to deal with the personal data breach and, where appropriate, of the measures **LIC** has taken to mitigate any possible adverse effects.

- In light of the tight timescales for reporting a breach, **LIC** shall adopt a robust breach detection, containment, management and mitigation policies and procedures in place.

The duty to notify an individual about a breach does not apply if:
LIC has implemented appropriate technical and organisational measures which were applied to the personal data affected by the breach; LIC has taken subsequent measures which will ensure that any high risk to the rights and freedoms to individuals is no longer likely to materialize; or it would involve disproportionate effort.

VII. DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)- Practical Approach to Risk & Impact Management For GDPR Compliance

- **LIC** shall achieve the security of data through the implementation of proportionate physical and technical measures called **data protection impact assessments (DPIAs)**. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

- **LIC** shall Identify threats that could do harm and thus indirectly affect its assets. Such threats could be intruders, breaches, criminals, and even disgruntled employees.

- **LIC** shall identify and rank the value, sensitivity, and criticality of data by determining the level of risk that data carries if threatened**.**

- **LIC** shall adopt DPIAs **at the early stages of any project including CCTV in order to find and fix problems, reduce the associated costs and damage to reputation that might otherwise accompany a data breach.**

- **LIC shall consider the nature, scope, context and purposes of the processing when deciding whether or not it is likely to result in a high risk to individuals' rights and freedoms.**

- **LIC** shall carry out a **DPIA** before processing personal data when the processing is likely to result in a high risk to the rights and freedoms of individuals. **DPIAs** shall be particularly relevant during **a privacy-by-design approach;** when LIC introduces a new data processing system or technology. Processing that is likely to result in a high risk includes (but is not limited to) **e.g. using new technologies (for example surveillance systems).**

- A **DPIA** that **LIC** shall carry out would contain the following:

  - ❖ A general description of your processing operations and the purposes;

  - ❖ An assessment of the risks to the rights and freedoms of individuals;

  - ❖ The measures envisaged to address those risks;

  - ❖ The safeguards, security measures and mechanisms in place to ensure you protect the personal data; and

  - ❖ A demonstration of how **LIC** is complying with the GDPR, taking into account the rights and legitimate interests of the data subjects and any other people concerned.

- If LIC carries out a DPIA that identifies a high risk and that, all measures have been exhausted to reduce the risk; LIC shall consult the ICO first before going ahead with the

processing. **The focus is on the 'residual risk' after any mitigating measures have been taken.** The Information Commissioner would **then respond within six weeks**. **This timescale may increase by a further month, depending on the complexity of the processing an organisation intends to carry out.**

- **On the other hand if LIC's DPIA identified a high risk, and measures have been taken reduce the risk so that it is no longer a high risk, LIC shall not be obliged to consult the ICO.**

- **LIC shall put into place** effective risk management best practices that articulate the adverse effects **LIC** might suffer as a result of not being GDPR compliant. **Risks** involved might include **public relations (reputational risk) and financial risks**. Reputational damage could be worse as **LIC** might lose donors and service-users' confidence.

- **LIC shall adopt mitigation actions to counteract those risks e.g. training employees and assigning a Data Protection Officer (DPO). LIC** shall also apply cost-effective actions to mitigate or reduce risks.

VIII. MITIGATING RISKS

- **LIC** shall consider a wide range of risk mitigation measures, ranging from **pseudonymisation**, **data minimisation** and **security measures**, to various **data governance or oversight mechanisms.**

- The appropriate mitigation measures that **LIC** adopts would depend on context and shall be chosen on a contextual basis, considering the; **risks involved, cost of implementation, effectiveness of these measures, impact on the purposes, interests or benefits that are being pursued, reasonable expectations of individuals, transparency, and the elements of fair processing.**

- Although **risk mitigation does not mean the elimination of risk but the reduction of risk** to the greatest reasonable extent, given the desired benefits and reasonable economic and technological parameters, **LIC** shall make a reasoned and evidenced based decision whether to

proceed with processing in light of any residual risks; taking into account "proportionality" vis-à-vis purposes, interest and/or benefits.

- If an individual has given a valid consent to a processing activity by **LIC**, it shall be used as indication that he or she has agreed to the corresponding risk in appropriate contexts

IX. DATA DISPOSAL

- **LIC** recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

- All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

- All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

- As part of best practice, **LIC** will continually review its subscribers' databases so that we only include those who really want to be contacted. Not only will we be left with our most dedicated supporters, it will maximise interest and resources.

X. PENALTIES

- From **the 25th of May 2018,** very serious financial penalties may be applied by ICO for breaches of the law and failure to keep personal data safely and securely. These penalties could be sufficiently large to close down **LIC** hence everyone working at **LIC** is reminded to take data protection very seriously.

REFERENCES

1. **DPA vs GDPR what are the differences between these legislations www.atg-it.co.uk**

2. **Guide to the General Data Protection Regulation (GDPR) | ICO ico.org.uk**

3. **Will GDPR affect charities and non-profits? | Security | ACUTEC www.acutec.co.uk**

4. **The Risk-Based Approach in the GDPR: Interpretation and Implications iapp.org**

5. **Chapter 3 – Rights of the data subject | General Data Protection Regulation (GDPR) gdpr-info.eu**

LIC urges you to review the GDPR policy thoroughly, discuss any concerns with your line managers or head of departments who will then forward your concerns to the LIC Data Protection Manager.

Lewisham
ISLAMIC·CENTRE

GDPR DECLARATION

Everyone will certify their acceptance of the **General Data Protection Regulation Policy** by signing the **Declaration** that they have read and will abide by this **Policy**.

I, (Employee) _____), have read, understood and agree to abide by the **GDPR** policy and I understand that such adherence is a condition of my **employment** or **contract**. I understand that a violation of the **GDPR policy** may be grounds for termination or dismissal for just cause without notice or pay in lieu of notice.

Signed this **Day** _____, **Month** _____, **Year**_____.

_____

(Employee - Signature)

_____

Department

(This page must be signed and handed over to the centre coordinator for filing records)