Speakers of Life Community Interest Company
Data Retention Policy
05 July 2019

1. Introduction

This Policy sets out the obligations of Speakers of Life Community Interest Company, a voluntary religious organisation based in England, registered with Company number 12074412, at 5 Emblehope Drive, Gosforth, Newcastle Upon Tyne, Tyne And Wear, NE3 4RW, (hereafter referred to as "**SOL**") regarding retention of personal data collected, held, and processed by SOL in accordance with EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The GDPR also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

In addition, the GDPR includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

a) Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);

b) When the data subject withdraws their consent;

c) When the data subject objects to the processing of their personal data and SOL has no overriding legitimate interest;

d) When the personal data is processed unlawfully (i.e. in breach of the GDPR);

e) When the personal data has to be erased to comply with a legal obligation; or

f) Where the personal data is processed for the provision of information society services to a child.

This Policy sets out the type(s) of personal data held by SOL **[**for Regular mail-shots and information updates, Appointment bookings, Event ticketing**] AND/OR [**by the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

For further information on other aspects of data protection and compliance with the GDPR, please refer to SOL's Data Protection Policy.

2. Aims and Objectives

1.1 The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that SOL complies fully with its obligations and the rights of data subjects under the GDPR.

1.2 In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that excessive amounts of data are not retained by SOL, this Policy also aims to improve the speed and efficiency of managing data.

3. Scope

1.1 This Policy applies to all personal data held **[**by SOL**] OR [**by the carefully approved associate organisations only of SOL**] AND/OR [**for Regular mail-shots and information updates, Appointment bookings, Event ticketing.**] [**and by third-party data processors processing personal data on SOL's behalf**]**.

1.2 Personal data, as held by **[**SOL**] OR [**the above**]** is stored in the following ways and in the following locations:

a) **[**SOL's servers, located in The EU, The UK;**]**

b) **[**Third-party servers, operated by Bluehost and Hotmail, Samsung, Google, Facebook, Mailchimp and Dropbox and located in The EU and The USA;**]**

c) **[**Computers permanently located in SOL's premises at NOT APPLICABLE;**]**

d) **[**Laptop computers **[**and other mobile devices**]** provided by SOL to its employees;**]**

e) **THIS LINE DOES NOT APPLY**

f) **[**Physical records stored in 5 Emblehope Drive, Gosforth, NE3 4RW;**]**

g) **[**THIS LINE DOES NOT APPLY.**]**

4. Data Subject Rights and Data Integrity

All personal data held by SOL is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in SOL's Data Protection Policy.

1.1 Data subjects are kept fully informed of their rights, of what personal data SOL holds about them, how that personal data is used **[**as set out in Parts 12 and 13 of SOL's Data Protection Policy**]**, and how long SOL will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

1.2 Data subjects are given control over their personal data held by SOL including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict SOL's use of their personal data, **[**the right to data portability,**]** and further rights relating to automated decision-making and profiling **[**, as set out in Parts 14 to

20 of SOL's Data Protection Policy**]**.

5. **Technical and Organisational Data Security Measures**

1.1 The following technical measures are in place within SOL to protect the security of personal data. Please refer to Parts 22 to 26 of SOL's Data Protection Policy for further details:

a) All emails containing personal data must be encrypted;

b) All emails containing personal data must be marked "confidential";

c) Personal data may only be transmitted over secure networks;

d) Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;

e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;

f) Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;

g) Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient **[**or sent using Royal Mail Special Delivery**]**;

h) All personal data transferred physically should be transferred in a suitable container marked "confidential";

i) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from Mark Birch-Machin.

j) All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;

k) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of SOL or not, without authorisation;

l) Personal data must be handled with care at all times and should not be left unattended or on view;

m) Computers used to view personal data must always be locked before being left unattended;

n) No personal data should be stored on any mobile device, whether such device belongs to SOL or otherwise **[**without the formal written approval of Mark Birch-Machin and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary**]**;

o) **[**No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of SOL where the party in question has agreed to comply fully with SOL's Data Protection Policy and the GDPR;**]**

p) All personal data stored electronically should be backed up at regular intervals with backups stored **[**onsite**] AND [**offsite**]**. All backups should be securely stored OR encrypted;

q) All electronic copies of personal data should be stored securely using passwords and encryption;

r) All passwords used to protect personal data should be changed regularly and should must be secure;

s) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

t) All software should be kept up-to-date. Security-related updates should be installed **[**not more than one month**] OR [**as soon as reasonably possible after**]** becoming available;

u) No software may be installed on any Company-owned computer or device without approval; and

v) Where personal data held by SOL is used for marketing purposes, it shall be the responsibility of Mark Birch-Machin to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

The following organisational measures are in place within SOL to protect the security of personal data. Please refer to Part 27 of SOL's Data Protection Policy for further details:

a) All employees and other parties working on behalf of SOL shall be made fully aware of both their individual responsibilities and SOL's responsibilities under the GDPR and under SOL's Data Protection Policy;

b) Only employees and other parties working on behalf of SOL that need access to, and use of, personal data in order to perform their work shall have access to personal data held by SOL;

c) All employees and other parties working on behalf of SOL handling personal data will be appropriately trained to do so;

d) All employees and other parties working on behalf of SOL handling personal data will be appropriately supervised;

e) All employees and other parties working on behalf of SOL handling personal data should exercise care and caution when discussing any work relating to personal data at all times;

f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

g) The performance of those employees and other parties working on behalf of SOL handling personal data shall be regularly evaluated and reviewed;

h) All employees and other parties working on behalf of SOL handling personal data will be bound by contract to comply with the GDPR and SOL's Data Protection Policy;

i) All agents, contractors, or other parties working on behalf of SOL handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of SOL arising out of the GDPR and SOL's Data Protection Policy;

j) Where any agent, contractor or other party working on behalf of SOL handling personal data fails in their obligations under the GDPR and/or SOL's Data Protection Policy, that party shall indemnify and hold harmless SOL against

any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

6 Data Disposal

Upon the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

1.1 Personal data stored electronically (including any and all backups thereof) shall be deleted **[In the case of Windows-OS-based data,** securely using Windows Cipher tool based deletion methods OR, in the case of Wordpress-based data, using the WP Tools Erase Personal Data method**]**;

1.2 **[**Special category personal data stored electronically (including any and all backups thereof) shall be deleted **[In the case of Windows-OS-based data,** securely using Windows Cipher tool based deletion methods OR, in the case of Wordpress-based data, using the WP Tools Erase Personal Data method**]**

1.3 Personal data stored in hardcopy form shall be shredded and recycled.

1.4 Special category personal data stored in hardcopy form **shall be shredded and recycled.**

7 Data Retention

1.1 As stated above, and as required by law, SOL shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

1.2 Different types of personal data, used for different purposes, will necessarily be retained for different periods **(**and its retention periodically reviewed), as set out below.

1.3 When establishing and/or reviewing retention periods, the following shall be taken into account:

a) The objectives and requirements of SOL;

b) The type of personal data in question;

c) The purpose(s) for which the data in question is collected, held, and processed;

d) SOL's legal basis for collecting, holding, and processing that data;

e) The category or categories of data subject to whom the data relates;

f) {This Line Does Not Apply}.

1.4 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

1.5 Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within SOL to do so (whether in response to a request by a data subject or otherwise).

1.6 **[**In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the

public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.**]**

Data Ref.	Type of Data	Purpose of Data	Review Period	Retention Period or Criteria	Comments
Mailer	Name, Email contacts	Regular mail-shots and information updates	Annually	No longer than 6 years more than date of last required period.	Subjects who, having consented, then withdraw that consent will have their op-out recorded for compliance purposes. An annual removal of unnecessary data will be processed.
Appointment	Name, Phone number, email contact	Appointment bookings	Annually	No longer than 3 years more than date of last required period.	Data is recorded electronically for management of bookings. Consent forms are also stored offline as specified above. These will be safely retained for accountability and compliance purposes for no longer than 3 years.
Event	Name, contact information	event ticketing	Every 3 Months as required.	no longer than 3 months after the event takes place	Event attendees may be on other databases/lists but we will not automatically include event ticket data in those other databases/lists.

8 Roles and Responsibilities

1.1 SOL's Data Protection representative is Mark Birch-Machin , enquiries@speakersoflife.org

1.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, SOL's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the GDPR and other applicable data protection legislation.

1.3 **[The Board of Directors]** shall be directly responsible for ensuring compliance with the above data retention periods **[**throughout SOL**] OR [**within carefully approved associate organisations only **]**.

1.4 Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Data Protection Officer.

9 Implementation of Policy

This Policy shall be deemed effective as of 05 July 2019. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: Mark Birch-Machin

Position: Managing Director

Date: 05 July 2019

Due for Review by: 05 July 2019

Signature: