

GDPR Data Protection Policy

Date Agreed: 9 November 2021

Reviewed: Annually

Introduction

Sustainable Living Initiative (SLI) needs to gather and retain certain information about individuals in order to ensure the smooth running of the organisation on behalf of its members. This data protection policy has been introduced in order to comply with GDPR regulations introduced in 2018.

Personal data collected and retained by SLI includes: member/volunteer details as per sign up/renewal form, employee and trustee information and contact details for anyone with whom SLI has a relationship. This policy outlines how this personal data will be collected, handled and stored to comply with the law and has been written following Information Commissioner's Office (ICO) guidelines.

GDPR places emphasis on consent, accountability and transparency with regards to the collection, management and storage of personal data and SLI endeavours to comply fully.

Definitions

Personal data is viewed as any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people. (www.ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/)

Key Principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations and SLI will ensure that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- 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.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- The controller (i.e. SLI designated persons) shall be responsible for, and be able to demonstrate, compliance with the principles.

Consent

The GDPR is clearer that an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in) - It specifically bans pre-ticked opt-in boxes.

It also requires distinct ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

The GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time.

A contract is also a lawful basis to collect/store personal data because either they have asked you to do something before entering into a contract or to fulfil your contractual obligations to them (e.g. provide a quote).

You must keep records to evidence consent identifying: who consented, when, how and what they were told.

In order to comply with these regulations, SLI obtains consent in the Sign-up/Renewal form completed by all members to be contacted about any SLI matters. SLI will be using Mailchimp to store contact lists and send out monthly mass communications; there always is an opportunity to unsubscribe at any time. All these actions are recorded and evidenced by Mailchimp and the deletion process instantaneous.

Individual Rights

The GDPR provides the following rights for individuals:

1. The right to be informed – individuals must be informed about the collection and use of their personal data as well as the purpose for processing, retention period and who it will be shared with.
2. The right of access - individuals have the right to obtain confirmation that their data is being processed and access to their personal data (information is to be provided free of charge and within one month unless requests are found to be unfounded, excessive or repetitive).
3. The right to rectification – individuals have the right to request inaccurate data to be corrected either verbally or in writing. This must be done within one month.
4. The right to erasure – Individuals have 'the right to be forgotten' unless data must be kept for legal reasons. Requests can be made verbally or in writing and organisations have one month to respond and react.
5. The right to restrict processing – individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances.
6. The right to data portability – allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data.
7. The right to object – individuals have the right to object to process based on legitimate interest, direct marketing and processing for purposes of scientific/historical research and statistics.

8. Rights in relation to automated decision making and profiling – individuals must explicitly consent to have their data used for automated decision making and profiling.

Accountability and Governance

SLI agrees, in accordance with GDPR regulations, to demonstrate and evidence its compliance to the above principles and recognises our responsibility and accountability.

SLI will demonstrate compliance by:

- Implementing appropriate measures and will ensure all employees, designated SLI representatives and volunteers comply with our internal Data Protection Policy.
- Regular reviews of the data we hold and record yearly data destruction cycles in October to remove the details of any member who does not renew their membership.

Storage of Data

Contact lists for mass communication will be stored on Mailchimp (www.mailchimp.com).

SLI Membership lists including Bluebell and Marlpit community gardens will be shared only with SLI staff, Trustees and designated coordinators (only name, e-mail address and skills) on Gdrive.

Paperwork containing personal data and sensitive information is to be kept in locked filing cabinets with access that is restricted to SLI staff or in the case of their absence a named Trustee of SLI. The cabinet is stored in a locked office with keys only available to staff or two named Trustees in the absence of staff e.g. Holidays, sickness.

Communication on behalf of SLI will only be undertaken using one of the designated 'grow-our-own' email addresses, not using a personal email address and access will only be given to staff or in their absence a Trustee or a designated person for example, coordinator.

Data Breaches

As per ICO instruction, SLI will report any data breaches within 72 hours to ICO and to the board of Trustees in order to undertake immediate action to remedy the breach.