GDPR Policies and Procedures

Policy owner Carrie Cort

Legislation and regulation UK General Data Protection Regulation (UK GDPR)

Formally endorsed by Trustees

Last update 20 July 2023

Next review

1. Introduction

Sussex Green Living (SGL) collects and uses data for a variety of purposes about its trustees, volunteers, employees, partners, donors, supporters and other individuals who come in contact with the organisation.

tailored by the Data Protection Act 2018 and supersedes the previous Data Protection Act 1988 and the Data Protection (Amendment) Act 2003.

The new Regulation aims to standardise data protection laws and processing across the EU and UK; affording individuals stronger, more consistent rights to access and control their personal information.

SGL is registered with the ICO (Information Commissioners Office). We have appointed a Data Protection Officer (DPO) who is registered with the ICO and who is the point of accountability for personal data in SGL. Staff and volunteers should consult with the DPO if in any doubt about the collection, use, and securing of personal data. Our DPO is currently Carrie Cort (cort@sussexgreenliving.co.uk).

2. Purpose of this document

This document is intended to:

- State SGL's commitment to protect the rights and privacy of individuals in accordance with the UK General Data Protection Regulation.
- Specify any rules, processes and procedures defined by SGL for handling personal data and fulfilling obligations relating to personal data.
- Serve as a guide for SGL staff and volunteers, describing our obligations as an organisation and how we will ensure those obligations are met.

3. Our obligations

This section describes the data privacy framework within which SGL operates, and SGL's obligations under that framework. Like all other UK organisations, we are governed by the

3.1 Regulatory framework

Personal information in the UK is regulated under the terms of the Data Protection Act 2018 (the DPA), which controls how organisations use personal information. The DPA is the UK's implementation of an EU regulation, the General Data Protection Regulation (GDPR). The body, within the UK, responsible for enforcing and clarifying the DPA is the Information Commissioner's Office (ICO).

Generally, the term 'GDPR' is used to refer to the set of rules that governs usage of personal information in the UK. The ICO provides an extremely useful body of information about GDPR, found at https://www.gov.uk/data-protection.

3.2 Definitions used in UK GDPR Policy

• Data means automated and manual data. Automated data means any information on computer, or information recorded with the intention that it be processed by computer. Manual data means information that is recorded as part of a relevant filing system or with the intention that the data form part of a system.

• Data Controller means a body that, either alone or with others, controls the contents and use of personal data.

• Data Processor means a person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment.

• Data Subject means an individual who is the subject of personal data.

• Personal Data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

• Processing means performing any operation or set of operations on the information or data, whether or not by automatic means, including:

a) Obtaining, recording or keeping the information, or
b) Collecting, recording organising, storing, altering or adapting the information or data,
c) Retrieving, consulting or using the information or data
d) Disclosing the information or data by transmitting, disseminating or otherwise making them available, or
e) Aligning, combining, blocking, erasing or destroying the information or data.

Relevant Filing System means any set of information relating to individuals to the extent that, while not computerised, is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Sensitive Personal Data means personal data, which relate to specific categories defined as:
a) The racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject,
b) Trade union membership
c) The physical or mental health or condition or sexual life of the data subject
d) The commission or alleged commission of any offence by the data subject, or
e) Any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

3.3 An organisation's responsibilities under the UK GDPR Policy

Any organisation holding personal information has certain key responsibilities in relation to the information which is kept on computer or in a structured manual file about individuals. These are summarised in terms of eight "Rules" which are listed below;

• Obtain and process the information fairly
• Keep it only for one or more specified and lawful purposes
• Process it only in ways compatible with the purposes for which it was given to you initially
• Keep it safe and secure
• Keep it accurate and up-to-date

• Ensure that it is adequate, relevant and not excessive
• Retain it no longer than is necessary for the specified purpose or purposes
• Give a copy of his/her personal data to any individual, on request.

3.4 An individual's rights under the UK GDPR Policy

Under the Data Protection Act 2018, an individual has the right to find out what information the government and other organisations store about them. These include the right to:

- be informed about how their personal data is being used
- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of your data
- data portability (allowing you to get and reuse your data for different services)
- object to how your data is processed in certain circumstances

An individual also has rights when an organisation is using their personal data for:

- automated decision-making processes (without human involvement)
- profiling, for example to predict their behaviour or interests

3.5 The ICO's set of GDPR principles for organisations

The ICO provides a useful and realistic set of principles for organisations to use in the handling of personal data. These are found at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/.

4. SGL's responsibilities

This section is a summary of the specific responsibilities of SGL and its staff and volunteers.

4.1 Overview

Within SGL, the DPO has overall responsibility for ensuring compliance with GDPR. However, all members, volunteers and employees of the organisation who collect and/or control the contents and use of personal data are also responsible for doing so in accordance with GDPR and with SGL's policies and procedures.

The organisation will provide support, assistance, advice and training to all members, volunteers and employees who handle data to ensure it is in a position to comply with UK GDPR.

It will be the responsibility of the DPO to develop and encourage good data handling practice within the organisation.

Volunteer data is an important element of the UK GDPR policy and all support volunteers and employees must be fully aware of the responsibilities in this matter and how they receive and store volunteer data. Please make sure to adhere to GDPR at all times when handling volunteer data.

4.2 Principles

The ICO principles are relevant to all organisations, but it is worth highlighting some of those that may be particularly relevant to SGL's operations:

- Purpose limitation: SGL should be aware of and be able to state the basis on which SGL is storing or using personal data.
- Data minimisation: SGL should hold no more data than is actually required for the specified purpose. Furthermore, systems and individuals in SGL should be granted access to no more data than they require.
- Integrity and confidentiality: SGL must appropriately secure data, to reduce the chance and severity of 'data loss', i.e. the leaking of data to unauthorised parties.

SGL is a small enough organisation that many GDPR obligations, such as the obligation to document processing in detail, do not fully apply to it. However, SGL should still maintain a catalogue of personal data held, a justification for holding and processing that data, and a basic set of policies (see below).

4.3 Personal data held by SGL

SGL holds personal data for several categories of individuals, including:

- Contact and other information about our own staff and volunteers. This information is collected with permission and used because it is essential to SGL's core activities.
- Information about donations, grants, events, and other activities; this information can often contain personal data, such as the contact information of third parties involved in a grant process.
- Publicity materials, which may include photos, videos, and other materials that identify individuals.

Generally, where information is *not* vital for SGL's ordinary activities, the justification for retaining and using it is the consent of the individual involved. This consent needs to be actively obtained, and can be withdrawn by the individual at any time. Photo and video information used in promotional material is likely to be seen as more sensitive, and specific consent should be sought and recorded for such use.

4.4 SGL's data storage systems

Data is held in Mailchimp, Eventbrite, Capsule, Calendly and Google Sheets. Only the CEO and authorised volunteers and employees have access to the data held in these systems. Authorization must only be granted to appropriately trained and trusted personnel and only as necessary to fulfil the stated purpose of the data processing.

SGL staff and volunteers must *not* store personal information (other than their own) on their local devices such as phones and computers; doing so will make it difficult for SGL to prevent data loss events and difficult for SGL to comply with GDPR rights requests.

6. Procedures

This section describes procedures to be followed in handling personal data. These procedures are lightweight, given the size of SGL; in the event of doubt, staff and volunteers should refer to the DPO.

6.1 Authorisation of staff and volunteers

Before being given access to SGL systems containing personal data, staff and volunteers shall:

- Read and understand this document and SGL's privacy policy (https://www.sussexgreenliving.org.uk/privacy-policy/)
- Have the opportunity to discuss any questions or concerns about their processing of personal data with the DPO
- Sign a declaration to SGL that they understand the policies and procedures, and SGL's obligations under the GDPR, and will abide by them.

Access to personal data will then be authorised by the DPO.

6.2 Keeping track of data and authorisation

SGL shall maintain a register of data assets, indicating those which contain personal and/or sensitive information, and a register or individuals authorised to access those assets. These registers will be updated by the DPO or someone appointed by the DPO when new data assets, or new staff, are added. Authorisations shall be reviewed periodically, and those permissions no longer required shall be revoked.

6.3 Data Protection Impact Assessment process

The ICO specifies that organisations conduct a Data Protection Impact Assessment (DPIA) when changing the way they process private data, when such a change is 'high risk'. Given the small size of SGL it is not

appropriate to define a comprehensive review process and it is not likely that SGL's processing is 'high risk' in ICO terms.

However, in order to ensure that SGL retains an awareness of the personal data it controls, SGL shall conduct an informal review of any new data asset or process, in which the new asset will be added to the register (if appropriate) and the DPO will satisfy themselves that the new data or process is suitably managed and poses minimal risk to individuals.

6.4 GDPR rights exercise process

The GDPR specifies various rights that the individual may choose to exercise, concerning their own personal data – for example, the right to be forgotten. The ICO provides a list of such rights here: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/. An organisation holding personal data needs to be prepared to facilitate these rights by responding in an effective and timely manner when an individual exercises them.

The process shall be as follows:

- The request is brought to the attention of the DPO.
- The DPO records the request, including the identity of the individual making it, the date, and the type of request.
- The DPO responds to the individual, letting them know the request has been received.
- The DPO has one month to action the request from the date on which the request is received.
- Depending on the type of request, the DPO will reach out to the owners of individual data assets and request the information pertaining to the individual. For an SAR (Subject Access Request), a report on the information will be returned to the individual; for an erasure request, confirmation that the individual's personal information has been erased from each asset will be returned.
- The DPO will inform the individual when the request has been actioned.

Because almost all GDPR rights are much more easily handled when information is kept in a centralized and catalogued form, SGL should avoid the storage of personal data anywhere not contained in the DPO's register – including individual's personal devices.

6.5 Data breach process

A 'personal data breach' in GDPR terms is an incident in which personal data is accidentally or unlawfully destroyed, altered, disclosed, or lost.

In the event of a data breach, the following process shall be followed:

- The discoverer of the breach shall notify the DPO.
- The DPO shall apply the standard ICO breach assessment checklist (https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/).
- If the assessment shows that there is a 'risk to people' involved, the DPO must inform the ICO within 72 hours of the discovery of the breach. Given SGL's size, it is unlikely that a material risk in ICO terms will be found, but the check shall be made anyway.
- The breach shall be recorded in a register, giving:
  - The nature of the breach
  - How and when it was discovered
  - Who was, or may have been, effected
  - Steps taken to resolve the issue and prevent re-occurrence

6.6 Annual Review

This document, the Privacy Policy, the data asset and authorisation registers, and any other assets and documents relating to personal data shall be reviewed annually by the Trustees, and updated as necessary in the light of changes to either the organisation or the regulatory requirements.

7. Status of this Policy

This policy has been approved by the Trustees and applies to all members of the organisation. All appropriate support volunteers and employees of SGL who have access to data must read, understand and adhere to this policy.

Any breach of this policy will be taken very seriously.

Any member of the organisation who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the DPO immediately.

8. Related information

Our Privacy Policy details how personal data is collected, used, stored and disposed of and can be viewed here https://www.sussexgreenliving.org.uk/privacy-policy/

9.Review

This Policy will be reviewed in light of any legislative or other relevant indicators in line with the UK General Data Protection Policy Regulation 2018 as set out by the Data Protection Commission.

Note of changes made	Date changes made	Date policy statement approved by the Trustees
Approved by the Trustees, except the Complaint handling policy statement		5th July 2022
Complaint handling policy statement		
Approved by the Trustees		

Sussex Green Living, The White House, Coneyhurst, Nr Billingshurst, West Sussex, RH14 9DH
W: SussexGreenLiving.org.uk
Registered charity 1189569