

SDCE Data Protection Policy

Introduction

SDCE takes data security very seriously and will collect, hold and process the minimum amount of personal data necessary to undertake its activities, in accordance with the six principles of the General Data Protection Regulations (GDPR). Personal data will not be passed onto third parties for the purpose of direct marketing.

1. Information we hold and legal basis for collecting and processing it

Directors' data

To meet the legal obligations of the Co-operative and Community Benefit Societies Act 2014 we must keep a register of Directors of the society. We are also legally required to provide details of our Directors to the Financial Conduct Authority. We therefore collect and hold the following personal data about our Directors:

- Name, home address, email address and telephone number(s)
- The date they became a director and the date they ceased to be a director.
- Date of birth.
- Other directorships.

Customer data

To provide a home energy advice service to residents in the South Hams and to meet the terms of grants we receive, we have a legitimate interest in collecting and holding the following information on those who contact us for help:

- Name, address, e-mail, phone numbers
- Tenancy status
- If they are over 65 years old
- If they receive benefits
- If they have access to the internet
- If they are in poor health

We only collect the minimum amount of information on the people that we help. The customer data is collected in a number of ways including;

- Event sign in sheets
- Paper notebooks/diaries used by our energy advisors
- E-mail, directly from clients or from third parties making referrals on clients' behalf
- Recorded telephone messages that are e-mailed to us
- The 'Contact us' form on our website

Supporter Data

To help us to demonstrate that our activities are community led and community focussed we invite local people to join us as supporters. These supporters give their consent to be kept informed of our activities, which is the legal basis for us processing their data. We hold the following personal data on our supporters: Name, e-mail, and occasionally phone numbers and addresses. Supporter data is collected by;

- Event sign in sheets
- E-mail directly from the prospective supporter
- The 'contact us' form on our website
- SurveyMonkey surveys

Member Data

To meet the legal obligations of the Co-operative and Community Benefit Societies Act 2014 we must keep a register of Members of the society. We therefore collect and hold the following personal data about our Members:

- Name, address, email and possibly phone number(s)
- If they are over 16 years old
- The date they joined us

Media and Group Contacts

To promote our service and make links with local groups we have developed and hold a list of local media and group contacts. This data is collected as it is in the legitimate interest of the society and includes the following personal data for the main contacts/editors:

- names, e-mails and phone numbers

2. Where we hold the data and for how long

Director data

The personal data about our Directors is held in the Company Register in electronic spreadsheet form. This is held in [Dropbox](#) and is password protected. We hold this data for up to 2 years after a Director leaves the society.

Customer data

Customer data is held in a variety of locations depending on how the original enquiry is made to us and how we respond to the enquiry. The majority of customer data is held in electronic spreadsheet form, which are password protected and stored in Dropbox. Only our two energy advisors have access to these. All letters or reports containing personal data are stored in specific folders on the SDCE laptop or our Energy Advisors home computer. These records and spreadsheets will be kept for up to 10 years.

Enquiries or client referrals made via e-mail, including voice messages from our Freephone number provider and our website 'contact us' form, are stored for as long as necessary to respond to the enquiry and are then deleted. Our Freephone service provider ([Telecommsworld Plc](#)) and our website host ([Weebly.com](#)) do not store the personal information that passes through them to SDCE. Our e-mail provider is [Gmail](#) and access to our inboxes is password protected. When sending reports to our funders or making referrals to third parties of behalf of clients the information is anonymised when possible and large files are sent via '[WeTransfer](#)'. The SDCE laptop and Energy Advisors computer(s) all require login passwords and have their security systems regularly updated to help keep their contents secure.

Paper sign in/event forms are held in a lockable folder at our energy advisors' residences. For grant audit purposes these have to be kept for up to 10 years. Paper notebooks and diaries containing client information are stored at our energy advisors' residences and shredded after 1 year.

Supporter Data

Personal data about our supporters collected on paper forms is stored at our official address in a lockable cabinet. The data is also input into a spreadsheet, which is held in Dropbox and is password protected. The e-mail addresses are input into a [Mailchimp](#) contact list so that the supporters that have given consent, can be sent our e-newsletters. Should a supporter no longer want to be a supporter of the organisation we will remove them from our spreadsheet and mailing list.

Supporter enquiries made via e-mail and our website 'contact us' form, are stored in our Gmail account until we have dealt with the enquiry and are then deleted.

Occasionally we use [Survey Monkey](#) to gather the community's views. Any personal data collected from these surveys is held within SurveyMonkey, until we have completed the research and it is then deleted. If the people completing the survey give their consent to be kept informed of our activities, we will store their contact details on our Supporter spreadsheet.

Member Data

The personal data about our Members is held in the Company Register in electronic spreadsheet form. This is held in [Dropbox](#) and is password protected. We hold this data for 1 year after a Member leaves the society. The paper application forms are held in a lockable cabinet at our official address for as long as the person remains a Member.

Media and group contacts

The data for our media and local group contacts is held in a spreadsheet in Dropbox and is updated as and when we are advised of new contact details.

3. Individual Rights

We are committed to protecting the privacy of the people we come into contact with and to working within the boundaries of the GDPR. There are seven specific rights that are issued to individuals by the GDPR, and we acknowledge our responsibility in providing those rights.

Right to be informed

Individuals have the right to be informed about the collection and use of their personal data. When speaking to a client we will explain what information we will keep on them, the basis for doing so and how long we will keep it for. This policy and our Privacy Policies are also available on our website and in paper format should a client or supporter request a hard copy.

Right of access

We will respond promptly to an individuals' request to access their personal data, taking reasonable means to verify the identity of the person making the request. We will provide information in the form of a spreadsheet, on paper or in a common electronic form, within 1 calendar month of the request. We cannot charge for this, but may charge a reasonable fee to cover administration costs if the request is manifestly unfounded, excessive or repetitive.

Right to rectification and data quality

We ensure that the personal data we hold on our Directors and Supporters remains accurate and up to date. Directors and Supporters are reminded regularly to notify the Society if their details change.

Requests from individuals to have their personal data corrected will be met within 1 calendar month and we will take reasonable means to verify the identity of the person making the request. Requests can be made verbally or in writing to the Company Secretary and will be dealt with by the Company Secretary.

Right to erasure including retention and disposal

Customers and Supporters have the right to be forgotten and can request the erasure of personal data either verbally or in writing to the Company Secretary. We will deal with these requests within one month, taking reasonable steps to verify the identity of the person making the request. We will notify any third parties that have received the personal data from us about the need for erasure.

Right of restriction

Customers and Supporters have the right to request the restriction or suppression of their personal data, which means that we can store it but not process it in any way. These requests can be made verbally or in writing to the Company Secretary and we will deal with them within 1 month. We will take reasonable steps to verify the identity of the person making the request and will try to resolve any issue that has led to this request. We will notify any third parties that have received the personal data from us about the need for restriction.

Right to data portability

Directors, Customers and Supporters can ask us to move, copy or transfer their personal data from one IT environment to another in a safe and secure way, without hindrance to usability. Requests will be handled by the Company Secretary within 1 month and will be free of charge. Personal data from the Company Register will be transferred in a structured, commonly used and machine readable format such as a CSV and XML file. Such files to be password protected with the password sent separately.

Right to object

We recognise an individual's right to object to the processing of their personal data for "legitimate interests". On receipt of an objection, we will assess whether the individual's grounds for objection relates to "his or her particular situation" and stop any data processing unless we can demonstrate compelling, legitimate grounds to continue which override the interests, rights and freedoms of the individual; or if the processing is for the establishment, exercise or defence of legal claims.

4. Governance and Accountability

The Society is not legally required to have a Data Protection Officer (DPO) but the role of data protection lead is taken by SDCE Director, Katie Reville, who will work closely with the Company Secretary should an individual make a request regarding their data under the GDPR. Their task is to:

- inform and advise the Board of its obligations to comply with the GDPR and other data protection laws

- monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities and processes
- train staff and conduct internal audits

Data processor contracts

SDCE does not employ a data processor and only two members of the SDCE team have access to personal data.

Data Protection by Design

SDCE will adhere to the principle of data protection by design, by using measures such as data minimisation and anonymisation. When designing a new project, personal data collection will be thoroughly thought through.

Data Protection Impact Assessments (DPIA)

SDCE will carry out a DPIA when introducing new technologies or if processing is likely to result in a high risk to the rights and freedoms of individuals.

Data Security

Keeping the personal data that we process secure is incredibly important to us. The GDPR requires that personal data shall be: 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 following list sets out the data security measures taken by SDCE

- The SDCE laptop and Energy Advisors' computer(s) require login passwords and have up to date security systems. They are not loaned to anyone outside of the organisation and do not have personal data sets saved directly onto their hard drives. They are not left unattended in vehicles or at events.
- SDCE will collect the minimum amount of personal data necessary to provide the service to our customers and to meet our reporting obligations to funders.
- SDCE Project Workers will avoid making unnecessary duplicate lists of personal data and will anonymise data when writing funding bids or activity reports.
- Personal data sets held by SDCE will not be stored on portable memory sticks.
- Paper copies of event sign in sheets, supporter forms, notebooks and diaries will be stored securely at our Energy Advisors homes and destroyed within a year, unless funder obligations require us to keep them longer for audit purposes.
- Project workers will not record personal data in notebooks and diaries unnecessarily when working with clients to reduce the risk of data being accessed unlawfully.
- Only the company secretary has access to the supporter and member contact details within our Mailchimp account to produce our e-newsletters.
- E-mails sent on behalf of SDCE are only sent using an @southdartmoorcommunityenergy.org email account and sent Bcc if more than one person is being sent the message. The e-mails carry a disclaimer explaining the confidential nature of the message and the action to take if someone receives it in error. Access to our e-mails is password protected.
- When e-mailing a third party regarding a customer, the customer must have given consent for the message to be sent and the minimum amount of personal data should be included in the message. The project worker should doublecheck that they are sending the message to the right person.
- We do not collect, store or otherwise use, any data on people who visit our website, twitter account or Facebook page.

International transfers

SDCE uses external IT services to store data ([Dropbox](#)), send and receive e-mails ([Gmail](#) and [WeTransfer](#)) and to send e-newsletters (Mailchimp). We are confident that although these service providers are based outside of the EU that they will comply with the GDPR by 25.5.18 and that our data is as secure as it can be. We have signed a supplementary data protection addendum with Mailchimp to give our data protection to the level of GDPR.

Breach notification

Should SDCE become aware of a personal data breach (i.e. the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data) the Board will assess if it is likely to result in a risk to the rights and freedoms of individuals. If this is the case, then the ICO will be informed within 72 hours. If the breach is likely to result in a high risk to the rights and freedoms of the individuals, then we will notify those concerned directly and without undue delay.

Annual Review

This policy will be reviewed annually, approved by the Board of Directors and issued to Directors and Officers who implement the policy.

Contacting us

To make a request under GDPR regarding your personal information please contact the Company Secretary by one of the following means;

Phone: 0800 112 3044

Write to: SDCE, 8 Speakers Road, Ivybridge, PL21 0JP

E-mail: sophie@southdartmoorcommunityenergy.org

First version of this Policy produced in April 2018

Approved at the SDCE Board meeting held on 12.9.2018



Chairperson

Reviewed on:

Reviewed on:

Reviewed on: