General Data Protection Regulation 2018
(GDPR)
Policy & Procedure
Including Privacy Statement

Policy information	
Organisation	SPPOT, A Community Interest Company – the Data Controller
Scope of policy	If the policy applies to branches (including offices overseas) which the Data Controller is responsible for, or if it only applies to part of the organisation, this should be stated.
Policy operational date	1st June 2013
Policy prepared by	Data Protection Officer (Kerri Bee)
Date approved by Board/ Management Committee	1st June 2013
Policy reviewed date	1st April 2018

Introduction

Purpose of policy

- To protect clients, staff and other individuals
- To comply with the law
- To protect the organisation
- For good practice

Brief introduction to Data Protection Act 1998

Data Protection is about protecting individuals from the consequences of data being misused or handled badly. The Data Protection Act sits alongside other legislation that tells us to look after the people we work with – in areas such as health and safety, child protection, discrimination, consumer protection and so on. The Data Protection Act is generally written so that it should never need to be used as a reason for doing something harmful. This does not mean that the right course of action is always clear, however, especially when it's a matter of balancing several different people's interests. If preventing harm is the top priority, demonstrating respect for the individual comes a close second. In our information-rich society, organisations (and even individuals) can behave in intrusive, unpleasant or annoying ways if they use data without the knowledge, or against the wishes, of the individual.

The 1998 Data Protection Act affects almost all voluntary organisations. However, many struggle to understand it, and worry that they might get into trouble by not complying. Or they take an over-cautious approach and allow their work to be hampered by unnecessarily tight restrictions. This guide aims to demystify the Act and give you a

framework for managing the data you encounter during your voluntary or paid work with SPPOT.

No organisation can afford to alienate people by behaving in ways they find unacceptable. These two themes: preventing harm and respecting the individual, run through the Act in many areas, in the Data Protection Principles Before going on to discuss how to satisfy the Principles, however, we need to look at exactly what information we are talking about.

Data Protection Principles

Everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is necessary
- handled per people's data protection rights
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection

There is stronger legal protection for more sensitive information, such as:

- ethnic background
- political opinions
- religious beliefs
- health
- sexual health
- criminal records

Policy statement

SPPOT is committed to

- complying with both the law and good practice
- being respectful of individuals' rights
- being open and honest with individuals whose data is held
- providing training and support for staff who handle personal data, so that they can act confidently and consistently
- Notifying the Information Commissioner voluntarily, even if this is not required.

Key Risks

- information about individuals getting into the wrong hands, through poor security or inappropriate disclosure of information
- individuals being harmed through data being inaccurate or insufficient

Responsibilities

Board of Directors
The Board of Directors has overall responsibility for ensuring that the organisation complies with its legal obligations.

Data Protection Officer
This is currently the Operations & Development manager.

Their responsibilities include:

- Briefing the board on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Notification
- Handling subject access requests
- Approving unusual or controversial disclosures of personal data
- Approving contracts with Data Processors

Specific Other Staff & Volunteers

The team is currently very small and so every staff member and volunteer has significant Data Protection responsibilities.

All staff and volunteers should be required to read, understand and accept any policies and procedures that relate to the personal data they may handle during their work.

Enforcement

Infringement of the Data Protection and related policies is dealt with through the disciplinary procedures.

Confidentiality

Confidentiality applies to a much wider range of information than Data Protection and we have a separate Confidentiality Policy.

Understanding of confidentiality

Normally access will to data be defined on a “need to know” basis; no one should have access to information unless it is relevant to their work.

This may be relaxed in the case of information which poses a low risk: for example, a list of business contacts may be made generally available, even if this means people having access who don’t strictly need it.

Communication

SPPOT staff and volunteers will be open and honest about all information we collect during our work. In practice this means that we will tell every person who we gather information about e.g. new staff, volunteers and customers:

- What information we need
- Why we need it
- Where it will be stored
- How long for
- Who has access to it
- How to exercise their rights in relation to it

SPPOT Staff and Volunteers will be trained in Data Protection as part of their Induction Training. Roles and responsibilities will be clearly explained during the induction and probation period.

Data Protection will form part of the ongoing dialogue between line managers and staff and volunteers. SPPOT seeks to continually improve its data protection procedures.

Authorisation for disclosures not directly related to the reason why data is held

These are in two main categories: those likely to be at the instigation, or in the interests, of the Data Subject, and those which are made during official investigations.

For the first (such as a financial reference request from a bank), consent from the Data Subject is likely to be the normal authorisation. This consent must be recorded. For the second, it may be appropriate for the Data Subject not even to be informed; authorisation should be sought from the Board of Directors.

Security Measures

Specific Risks

<u>Home working, home visits, community buildings, training courses, in meetings etc.</u>

SPPOT uses smartphones and laptops because our staff and volunteers often work from home and travel around many different types of environment and work alone too (see lone working policy). The following procedures are designed to protect data.

Data recording and storage

<u>Computers, Tablets, Smartphones</u>

SPPOT currently uses non-linked, portable laptop computers and 1 desktop computer plus smartphones for key staff.

The following must be followed:

1. Every device must be password protected.
2. Every user account on computers will be password protected.
3. Every application on the device that has access to sensitive or personal data will be password protected.
4. Passwords will be stored using encrypted systems – training will be provided.
5. Portable computers will not have ANY personal or sensitive information stored on them. If one were to be stolen, a hacker will not be able to access any personal or sensitive data.
6. All data will be saved on specific, cloud-based storage that has been checked and verified with reference to data protection and
7. All devices will be kept secure when not in use.
8. The Operations & Development Manager will ensure that the central desktop computer is regularly backed up to Cloud storage and two external hard drives.
9. The Operations & Development Manager will ensure that the central desktop computer is password protected and locked away when not in use.

Cloud Based Storage

SPPOT uses Cloud based storage and systems which have been checked for compliance with the data Protection Act as follows:

Google G-Suite is a world leader in safe data storage and we use this business class system for email, calendar, document storage and as a customer database, storing names and contact detail.

Google have a full GDPR Resource Centre here.

Smartsheet is the project management software that we use for all our administrative systems e.g. customer journey tracking, quality assurance, complaints and compliments management, human resources, health and safety, accredited training records.

Their latest GDPR compliant data protection policy, procedure and statement are online here

Supersaas is the system we use for online booking of training courses, referrals, job applications and so forth made through our website or via email. This connects to our website and Smartsheet.

Supersaas GDPR statement is here

Storage of paper records

Paper records will be kept to a minimum and under lock and key, with keys (signed in and out) given only to those staff who need it.

Paper records will be scanned and stored on the Google File Drive.

Storing Personal Data

SPPOT only keep personal data it needs for the time that it is needed. Every person is aware of what we keep, why, and who can see it at the point they engage with SPPOT.

When they disengage, we ask them to complete a form stating their personal data preferences. For example, many customers ask us to keep their email address to send newsletters. We then delete any other personal data we have and adjust how they are stored e.g. move the customer entry from 'dog walking customer' group to 'SPPOT Community;' contact group.

These systems ensure continual maintenance of the systems and in addition we conduct a quarterly sweep of all systems to double check we are not holding any personal information, past the point that the individual is involved with the organisation.

Subject access

Individuals have a right to know what information is being held about them.

In response to a valid request (including the fee, if required), the Data Controller must provide a permanent, intelligible copy of all the personal data about that Data Subject held at the time the application was made.

The Data Controller may negotiate with the Data Subject to provide a more limited range of data (or may choose to provide more), and certain data may be withheld. This includes some third-party material, especially if any duty of confidentiality is owed to the third party, and limited amounts of other material. ("Third Party" means either that the data is about someone else, or someone else is the source.)

Subject access requests must be in writing. There should be a clear responsibility on all staff to pass on anything which might be a subject access request to the appropriate person without delay.

Where the person managing the access procedure, does not know the individual personally they will checking their identity before handing over any information.

There is no charge for subject access and the required information will be provided "in permanent form".

Transparency

SPPOT staff and volunteers will be open and honest about all information we collect during our work. In practice this means that we will tell every person who we gather information about e.g. new staff, volunteers and customers:

- What information we need
- Why we need it
- Where it will be stored
- How long for
- Who has access to it
- How to exercise their rights in relation to it

SPPOT staff and Volunteers will be trained in Data Protection as part of their Induction Training. Roles and responsibilities will be clearly explained during the induction and probation period.

Data Protection will form part of the ongoing dialogue between line managers and staff and volunteers. SPPOT seeks to continually improve its data protection procedures

Note that there is no obligation to inform people of anything that is obvious from the context or from general knowledge, or to inform people whose data is obtained from a third party where the cost of informing them would be disproportionate to the risks of holding and using the data: a typical example might be business contact lists.

Consent

Underlying principles

Consent from the individual is how we comply with the Fair Processing Conditions. We will process data:

- only with consent
- preferably with consent, provided seeking it is practicable
- without seeking consent

Where data is being processed without consent it is still very important to ensure that the Data Subject knows what is being done. See 'Subject Access' also.

All consent will be recorded in writing or by checking a box in online forms.

Direct marketing

SPPOT only keeps personal data it needs for the time that it is needed. Every person is aware of what we keep, why, and who can see it at the point they engage with SPPOT.

When they disengage, we ask them to complete a form stating their personal data preferences. For example, many customers ask us to keep their email address to send newsletters. We then delete any other personal data we have and adjust how they are stored e.g. move the customer entry from 'dog walking customer' group to 'SPPOT Community;' contact group.

These systems ensure continual maintenance of the systems and in addition we conduct a quarterly sweep of all systems to double check we are not holding any personal information, past the point that the individual is involved with the organisation.

In addition, with every 'marketing' event, e.g. newsletter, call to action etc., we provide clear information on how to unsubscribe.

We also state that we do not share any personal information with any other party for marketing purposes.

Staff training & acceptance of responsibilities

Induction

SPPOT Staff and Volunteers will be trained in Data Protection as part of their Induction Training. Roles and responsibilities will be clearly explained during the induction and probation period. There is an online induction procedure to support the in-person training which records each staff member's and volunteer's 'sign up' to the policies and procedures.

Data Protection will form part of the ongoing dialogue between line managers and staff and volunteers. SPPOT seeks to continually improve its data protection procedures.

Date	Signature	Position

Privacy Statement: for website publication and in writing by email or on paper to all current and future customers

Privacy Terms and Disclosure 1. Data Protection

The information you have provided is subject to the General Data Protection Regulation (Regulation (EU) 2016/679). (GDPR)

By signing this document, you consent to us or any company associated with us, for example, product providers or platforms we use to provide you with our services, processing your personal data, both manually and by electronic means. Your data will be used for the sole purpose of providing financial advice, administration and management.

“Processing” includes obtaining, recording or holding information or data, transferring it to other companies associated with us, such as product providers, the FCA or any other statutory, governmental or regulatory body for legitimate purposes including, where relevant, to solicitors and/or other debt collection agencies for debt collection purposes and carrying out operations on the information or data.

In order to provide services to you we may be required to pass your personal information to parties located outside of the European Economic Area (EEA) in countries that do not have Data Protection Laws equivalent to those in the UK. Where this is the case we will take reasonable steps to ensure the privacy of your information.

The information provided may also contain sensitive personal data for the purposes of the Act, including information that relates to your physical or mental health or condition; the committing or alleged committing of any offence by you; any proceedings for an offence committed or alleged to have been committed by you, including the outcome or sentence in such proceedings.

If at any time, should you wish to withdraw consent, for us or any company associated with us, to processing your personal data or sensitive personal data, please contact The Data Protection Controller: Kerri Bee, Operations and Development Manager, at SPPOT DHQ, Furzy Park, Haverfordwest, Pembrokeshire, SA61 1HT, enquiries@sppot.co.uk

You may be assured that we and any company associated with us will treat all personal data and sensitive personal data as confidential and will not process it other than for a legitimate purpose associated with the service we will provide you. Steps will be taken to ensure that the information is accurate, kept up to date and not kept for longer than is necessary.

If we provide you with financial advice, your data will be kept in accordance with FCA regulatory expectations, which in some cases mean the duration could be indefinite. Measures will also be taken to safeguard against unauthorised or unlawful processing and accidental loss or destruction or damage to the data. Subject to certain exceptions, you are entitled to have access to your personal and sensitive personal data that is held by us. You will not be charged for us supplying you with such data, however we do reserve the right to apply a ‘reasonable fee’ where requests are deemed excessive. We will respond to your request as soon as possible and within the maximum time frame of one month.

2. Data Processing

We will ensure that we are accountable and are able to demonstrate that data processing only occurs within the following principles:

1. Your data will be lawfully and fairly processed in a transparent manner. 2. Your data is collected on the grounds of explicit and legitimate purposes only. 3. We will only ask for your data when necessary, explain if data will be shared and how long it will be kept. 4. Your data will be accurate, kept up to date and erased, without delay, should your data no longer be required for the purposes to be processed. 5. Your data will only be retained for as long as is necessary. 6. Your data will be secure.

3. Rights of the client

The points below clearly set out the rights each client is entitled to. Please ask us for an explanation of each, should you wish to have more information.

1. The right to be informed. 2. The right of access 3. The right to rectification. 4. The right to erasure 5. The right to restrict processing 6. The right to data portability 7. The right to object. 8. Rights to automated decision and profiling.

4. Right to complain

In rare occasions where you believe your data has been wrongfully processed, stored or handled, you have the right to raise a concern with the Information Commissioner's Office (ICO).

Details on how to do this can be found here:

https://ico.org.uk/for-the-public/raising-concerns/

5. Communication and Marketing Preferences

Occasionally, SPPOT may send you marketing/promotional communications via email, telephone, SMS or the post. Recipients will be carefully selected, and information will only be sent where we feel it to be appropriate.

Please indicate YES or NO below:

I wish to opt IN to receiving communications or marketing material: YES/NO

If you consent to SPPOT contacting you for this purpose please tick to say how you would like us to contact you:

Post

Email

Text message (SMS)

Telephone

Should you wish to notify us electronically, please email us or SPPOT login and amend your preferences accordingly.

I hereby give consent to SPPOT for my personal data to be processed in accordance with the General Data Protection Regulations (GDPR) and in relation to the purposes described in Section 1 of this document.

Client Name:

Signed:

Date:

Client Name:

Signed:

Date: