General

Data Protection Regulation Act

28/05/2018

How It Affects You

Information Governance Document

Keep all Personal Data in the Same Way You Would Expect Others to Keep Your Data – Confidential

Awareness

The Data Protection Act 1998 has now been changed with the new General Data Protection Regulation (GDPR) applied on 25th May 2018.

The purpose of this Governance document is to help Support for Survivors Charity understand the rationale of the **General Data Protection Regulation Act, to** give our Charity practical steps we can take to ensure that **'Support for Survivors Charity data** is held securely and therefore, ensure we comply with the **(GDPR) act.** There are instances where information should or may be shared with other agencies and/or which will override the **GDPR** principles.

Child Safeguarding & Ongoing Protection Issues

Adult Safeguarding & Ongoing Protection Issues

Police inquiries (In the Interest of the public) on a need-to-know basis.

Benefits, Welfare, Housing Issues

NHS & Emergency

Your GP

HM Courts & Tribunals Services (HMCTS)

HM Revenue & Customs (HMRC)

GDPR 12 Steps

1. **Awareness**
2. **Information we hold.**
3. **Communicating privacy information.**
4. **Individuals' rights.**
5. **Subject access requests.**
6. **Lawful basis for processing personal data.**
7. **Consent**
8. **Children**
9. **Data breaches.**
10. **Data protection by design & data protection impact assessments.**
11. **Data protection officers.**
12. **International**

What is the General Data Protection Act?

The GDPR act places greater emphasis on the documentation that data controllers must keep demonstrating our accountability. Compliance with all the areas listed in this document will require SFS (Support for Survivors) Charity to review our approach to governance and how we manage data protection as a corporate issue. Some parts of the GDPR will have more of an impact on some organisations than SFS Charity.

Information We Hold

Personal data is information about you or one of our service users. It can be your/their, name, address, or telephone number, it can also include the information that our victims and survivors have provided concerning you. Support for Survivors needs this information so that we can identify and support the victim and survivor through their support of our charity.

For example, if an individual/s gave us inaccurate personal data **(and this has happened in the past),** and we have shared this inaccuracy with another organisation, we will have to tell the other organisation about the inaccuracy so they can correct their records. We will not be able to do this unless we know what personal data we hold, where it came from, and who we shared it with. **This inaccuracy must also be documented.** Doing this will help us to comply with the GDPR's accountability principle,

which requires us to be able to show how we comply with the GDPR protection principles. This will be effective with the Charities Policies and procedures.
Data controllers must make every effort available to ensure the information they use is accurate. This is because often the information held is sensitive and its inaccurate use could result in misrepresentation on behalf of the customer.

In other words – make sure your data is true. If any suspicion exists that the information is inaccurate, check with the individual.

Check with the individual.

GPDR also gives an individual a right of access to **'personal data.' This personal data** qualifies as any information held by the Support for Survivors Charity that relates to a service user. **Personal data** is collected when a service user completes their assessment. Though our referral process contains sensitive information, this can be sent from another organisation or the individual. It can consist of contact, and any other necessary details needed to facilitate an exchange.

However, much of the data that **Support for Survivors** collected is sensitive and if it were to fall into the wrong hands it could result in fraudulent activities against the individual. We regard this to be a direct breach of civil liberties.

With so much personal data held by an increasing number of organisations, there needs to be some benchmark for companies to follow if they are to ensure that data is handled fairly. **The General Data Protection Act** acts as a foundation for providing that benchmark.

Support for Survivors Charity needs to store personal data from clients to perform business activities and is classified as a **'data controller.'** As a **data controller, SFS** Charity must notify the **Information Commissioner's Office (ICO)** that **We** are responsible for the availability, integrity, and security of that data under the Act.

What is a Privacy Notice?

Support for Survivors Charity processes people's data, and we fall under the requirements of the General **Data Protection Act.** Some of the key regulatory bodies are responsible for promoting faithfulness to the **ACT.**

When we collect personal information data, we must give our service users certain information, such as our identity and how we intend to use their personal information. **(this is done through a privacy notice) under** the GDPR there are some additional things we will have to tell people. i.e., we will need to explain our lawful basis for processing activity. **(Service user/s will have a stronger right to have their data deleted where we use consent as our lawful basis for processing their personal information).**

The lawful bases in the GDPR are broadly the same as the conditions for processing in the 'Data Protection Act.'

What Privacy Information Should We Supply?

	Personal data Collected from Individuals	Personal data Obtained from Other Sources
SFS Name & contact details of SFS	Yes	Yes
Name & contact details of Representative	Yes	Yes
Name & details of our data Protection officer	Yes	Yes

The purposes of the processing	Yes	Yes
The lawful basis for the processing	Yes	Yes
The legitimate interests of the processing	Yes	Yes
The categories of personal data obtained	Yes	Yes
The recipients or categories of recipients		
The personal data	Yes	Yes
The details of transfers of personal data		
To any third countries or international Organisations	Yes	Yes
The retention periods for the personal data	Yes	Yes
The rights available to individuals with respect Of the processing	Yes	Yes
The right to withdraw consent	Yes	Yes
The right to complain with a Supervisory authority	Yes	Yes
The source of the personal data	Yes	Yes
The details of whether individuals are under A statutory or contractual obligation to Provide the personal data	Yes	Yes

Share Data (or sell it with) other Organisations.

- As part of the privacy information we provide, we must tell people who we are giving their information unless we are relying on an exception or an exemption.
- We can tell people the names of the organisations, or the categories that they fall within, and choose the most meaningful option.
- We do not sell personal data.

Information Support for Survivors Holds

- **Name**
- **Address**
- **Date of birth**
- **Telephone number and mobile number**
- **Email address**
- **Social media name and sites**
- **Status**
- **GP name, practice name and address**
- **National insurance number**
- **NHS Number**
- **Personal & sensitive information appertaining to victim & survivor assessment and disclosures**
- **Ethnic background**
- **Religious beliefs**
- **Gender**
- **Health & wellbeing**
- **Criminal Record/s**
- **Next of kin information**
- **Referrer information**
- **Personal information is given to the Trustees.**

Information We Share as a Collective

Meaning that all data we collect is necessary to complete the needs of the Charity and the victim's and survivors' support. As a charity, we will not ask for or hold any personal data that is outside of our concern.

Support for Survivors Charity will be in breach of the **General Data Protection Act** if we hold data irrelevant to our and the individual's purpose.

In other words – we as a charity must not be greedy. We will only collect data that we need to know and not any additional data that may be useful to us in the future.

The information must be processed by the Individuals 'Rights'

The GDPR includes the following rights for individuals.

The individual rights that this principle refers to include:

- The right to be informed.
- The right to access a copy of their information is held.
- The right to rectification.
- The right to erasure, block, or destroy.
- The right to restrict processing.
- The right to object.
- The right not to be subject to automated decision-making, including profiling.
- The right to prevent processing for direct marketing.
- A claim to compensate for damage caused by a breach of the act.
- The right to data portability (this is a new act, and it only applies).

To personal data, an individual has provided to a data controller.

Where the processing is based on the individual's consent or for the performance of a contract.

When processing is carried out by automated means,

In other words – give the individual access. It is the data we are holding. They should have a say in how it is used.

Practical Security Measures

It is All staff, volunteers, and trustee's responsibility to ensure they familiarise themselves with the relevant policies.
Shred all paper documents containing personal data once you have finished with them by national guidance.
Do not leave your computer unattended with Identifiable Information visible. Log off all systems when not in use.
Do not let others know or use your password.
Situate your screen so that information is not displayed to others.

Ensure sensitive, confidential, and personal data are not left situated where unauthorised people can read it.
Documents or mobile devices must not be stored in vehicles overnight and where transportation is required; the items must be in a car boot or out-of-sight storage area.
Do not discuss confidential information with others unless it is necessary for you or their job.
It should always be on a need-to-know basis and ensure all discussions are held where others cannot overhear you.

The most common breaches of data relate to data exposure – where a company or Organisation loses a computer device containing personal data. As well as the obvious distress this can have on the individuals involved.

This can also act as a significant black spot in SFS's reputation.

The ICO is also not averse to fining organisations responsible for negligence.

In other words – we must not be careless.

We must ensure all measures exist to keep the personal data we are responsible for out of the wrong hands.

The General Data Protection Requirements & Principles – Including Access & Security

- In most cases we will not be able to charge for complying with an access request.
- SFS Charity has one month to comply, rather than 40 days.
- SFS Charity can refuse a request, or charge for requests that are manifestly unfounded or excessive.
- If SFS Charity refuses a request, we must tell the individual why and that they have a right to complain to the supervisory authority and a judicial remedy.
- SFS Charity must do this without undue delay and, at the latest, within one month.

If SFS handles many access requests, we must consider the logistical implications of having to deal with requests more quickly and must consider whether it is feasible or

desirable to develop systems that allow service user/s to access their information easily online. **(In our Charities case, this would not be feasible).**

Information Consent

This means that any **personal data** collected by SFS Charity must be provided with the consent of the individual. This is commonly identified by written disclaimers in purchase contracts that are signed. To be acting fairly, the collecting charity must be transparent and ensure service users are fully informed and understand what will happen to their personal information.

In other words – we must be honest. We must gain permission to use any collected data and let the individuals know exactly what it will be used for.

Children

SFS does NOT need to bring any special attention to the protection of children, BUT if we have a concern, we must contact Children's Social Services or NSPCC.

Information Storage, Retention & Deletion

Victims & Survivors who have not engaged with us for 6 years:
(Please note some funders require us to keep information for longer)
(For legal purposes and for victims and survivors wishing to disclose information to the Police and civil prosecution, we will keep your information for longer)
If a Victim or Survivor draws consent, they can do this in any of the following ways: a letter to the 'Data Controller' Support for Survivors Charity, 'Woodthorpe House,' Mansfield Road, Sherwood, Nottingham, NG5 3FN.
Email director@supportforsurvivors.org
In person at the reception between 10:30 am and 4:00 pm, Monday to Friday

All your paperwork details will be shredded and deleted from the SFS database.

Individuals can change their contact preferences with us at any time by sending an email to director@supportforsurvivors.org with '**OPT OUT**' in the subject email field.

Individuals have the right to complain to the Information Commissioner's office at www.ico.org.uk if they think there is a problem with the way we are handling their data.
The General Data Protection Act states that the Charity must not hold on to data for any longer than is necessary. i.e., **if the Charity were to keep a credit card detail several years after a contract has terminated.**

Support for Survivors is encouraged to conduct regular reviews of the personal data they hold and securely destroy any information that is no longer relevant.
In other words – we do not hoard. We only keep hold of old files if needed or if you are required to by law.

Data Breaches

SFS Charity must make sure that we have the right procedures in place for detection to report and investigate a personal data breach.

- POSSIBLY SOME OTHER BODIES.
- THE GDPR introduced a duty to all organisations to report certain types of data breaches to the ICO, and in some cases, to individuals.
- SFS must only report and notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals.

  This could be for discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage.

Where a **BREACH** is likely to result in a substantial risk to the rights and freedoms of individuals, we will also have to notify those concerned directly in most cases.

Examples

SFS suffered a breach that resulted in an accidental disclosure of one of our service users. There is most likely to be a significant impact on the affected service user because of the sensitivity of their data and their details become known to others. This is likely to result in a substantial risk to their rights and freedoms, so the service user must be informed of the breach.

SFS experiences a breach when one of the workers accidentally deletes a record of one of our service users. The service users' details are later re-created from a backup. This is unlikely to result in a substantial risk to the rights and freedoms of the service user. They do not need to be informed.

If we decide to notify an individual/s we will still need to notify the ICO unless we can demonstrate that the breach is unlikely to result in a risk to the rights and freedoms of the individual.

We need to remember that the ICO has the power to compel us to inform those affected individuals if they consider there is a substantial risk. We must always

document our decision-making process in line with the requirements of the accountability principle.

What Information must we provide when telling individuals about a breach?

We Need To.

- **Describe.**
- **Be clear.**
- **In plain language, the nature of the personal data breach and explains the following.**

1. **GIVE the name and contact details of our data protection officer. (Managing Director Maxi 'Leigh)**
2. **Contact – as highlighted in red above.**
3. **Description of the consequences of the personal data breach.**
4. **A description of the measures we are taking or proved to be taking.**
5. **We are dealing with the data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.**

Finally: -

SFS Charity must ensure that we record all breaches, regardless of whether we need to be reported to the ICO.

Article 33(5) of the GDPR Act requires us to document the facts relating to the breach, its effects, and the remedial action we are taking. This is part of our overall obligation to comply with the accountability principle and allows us to verify our charity's compliance with our notification duties under the GDPR.

As with any security incident, we must investigate whether the breach was a result of human error or a systemic issue and see how a recurrence can be prevented, whether this is through better processes, further training, or other corrective steps.

Checklists

SFS knows how to recognise a personal data breach.

SFS understands that a personal data breach is not only about loss or theft of personal data.

SFS has prepared a response plan for addressing any personal data breaches that occur.

SFS has allocated responsibility for managing breaches to a resolute person or team.

The SFS workforce knows how to escalate a security incident to the appropriate person or team member in our charity to determine whether a breach has occurred.

SFS has in place a process to assess the risk to individuals because of a breach.

SFS knows and is aware of who the relevant supervisory authority for our processing activities is.

SFS has a process to notify the ICO of a breach within 72 hours of becoming aware of the breach, even if we do not have all the details yet.

SFS has a process to inform affected individuals about a breach when it is likely to result in a substantial risk to their rights and

Volunteer Print Name:

Signature:

Date:

GDPR was created by Maxi 'Leigh (Founder Care Services Director

Signed: Maxi 'Leigh

Date: 29th August 2023

Sherwood Community Centre
Woodthorpe House,
Mansfield Road, Sherwood,
Nottingham, NG5 3FN

Charity Registered Number:
1165986

Email:
hello@supportforsurvivors.org
Telephone: 0115 926 2722
Web: www.supportforsurvivors.org