Support For Survivors

A Registered Charity supporting Male & Female
SURVIVORS of Childhood Sexual/Physical/
Psychological/Incest Abuse & Rape

General
Data Protection Regulation Act
28/05/2018

How It Affects You

Information Governance Document

First Approved by J.T 9th Dec 2011
Revised5th April 2017
Revised June 2018 (New GDPR Act came into place to override DPA)
Revised5th April 2019
Revised 5th April 2020
Updated 24th April 2021

Support for Survivors. Registered Charity Number 1165986
C/o Self Help Nottingham & Nottinghamshire
C/o The Carers Federation, 1 Beech Avenue, Sherwood Rise, Nottingham Ng7 7LJ
Tel: 0115 911 1661
info@selfhelp.org.uk
www.selfhelp.org.uk/nottinghamshire

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

Awareness

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

The purpose of this Governance document is to help Support for Survivors Charity to understand the rational 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 enquiries (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 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 organizations than Support for Survivors Charity.

Information We Hold

Personal data is information about you or one of our individual/s. It can be your/their, name, address, or telephone number, it can also include the information that our victims and survivors has provided concerning you. Support for Survivors need this information so that we can identify and support the victim and survivor throughout their support with 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 organization, we will have to tell the other organization about the inaccuracy so they can correct their own 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.** By 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 Support for Survivors Charity 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.

GPDR also gives an individual a right of access to **'personal data'**. **This personal data** qualifies as any information held by Support for Survivors Charity that relates to an individual. **Personal data** is collected when an individual completes their assessment, although our referral process and also contains sensitive information, this can be sent from another organization or from the individual themselves. 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 could result in fraudulent activities against the individual. This is regarded to be a direct breach of civil liberties.

With so much personal data held by an increasing number of organizations, 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 is classified as a **'data controller'**. As a **data controller Support for Survivors** 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 requirements of the General **Data Protection Act.** Some of the key regulatory bodies responsible for promoting faithfulness to the **ACT**

When we collect personal information data, we must give our victims and survivors 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. **(People 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
S4S Name & contact details of our Organisation	✓	✓
Name & contact details of us Representative	✓	✓
Name & details of our data Protection officer	✓	✓
The purposes of the processing	✓	✓
The lawful basis for the processing	✓	✓
The legitimate interests for the processing	✓	✓
The categories of personal data obtained		✓

The recipients or categories of recipients of The personal data	✓	✓
The details of transfers of the personal data To any third countries or international Organisations	✓	✓
The retention periods for the personal data	✓	✓
The rights available to individuals in respect Of the processing	✓	✓
The right to withdraw consent	✓	✓
The right to lodge a complaint with a Supervisory authority	✓	✓
The source of the personal data	✓	✓
The details of whether individuals are under A statutory or contractual obligation to Provide the personal data	✓	✓

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 to, 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, choose the option that is most meaningful.
- We do not sell personal data.

Information Support for Survivors Holds

- **Name**
- **Address**
- **Date of birth**
- **Telephone number & mobile number**
- **Email address**
- **Social media name & sites**
- **Status**
- **GP name, practice name and address**
- **National insurance number**
- **NHS number**
- **Personal & sensitive information appertaining to victim & survivor assessment & your disclosures**

- **Ethnic background**
- **Political opinion**
- **Religious beliefs**
- **Health**
- **Sexual health**
- **Criminal Record/s**
- **Personal information held to Trustees**

Information We Share as a Collective

Meaning that all data we collect is necessary to complete the needs of the Charity and the victims 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 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.

Information must be Processed in Accordance with the Individual's 'Rights'

The GDPR includes the following rights for Individuals

The individual's rights that this principle refers to include:

- The right to be informed
- The right of access to a copy of their information which is held
- The right to rectification
- The right to erasure, blocked, or destroyed
- 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 compensation for damaged 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 individuals 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 their 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 in accordance with 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 personal password.
- Situate your screen so that Information is not displayed to others.
- Ensure sensitive, confidential, and personal data is 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 your 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 Organization 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 on S4S's reputation.

- The ICO is also not averse to fining organizations 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.
- Support for Survivors Charity have one month to comply, rather than 40 days.

- Support for Survivors Charity can refuse a request, or charge for requests that are manifestly unfounded or excessive.
- If Support for Survivors Charity refuse a request, we must tell the individual why and that they have a right to complain to the supervisory authority and to a judicial remedy.
- Support for Survivors Charity must do this without undue delay and at the latest, within one month.

If S4S handles a large number of 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 individuals 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 Support for Survivors 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 company (Support for Survivors) must be transparent and ensure clients 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

Support for Survivors do NOT need to bring any special attention for the protection of children, BUT if we have a concern it is imperative that we contact children's social services or NSPCC.

Information Storage, Retention & Deletion

1. Victims & Survivors who have not engaged with us for 3 years:
   - (please note some funders require us to keep your information for longer)
   - (for legal purposes and Victims & Survivors wishing to disclose information to the Police and civil prosecution we will keep your information for longer)
2. 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 reception between 10:30am and 4:00pm Monday to Friday

All your paperwork details will be shredded and deleted from S4S database.

Individuals can change their contact preferences with us at any time by sending an email to davidnrobinsons4s@gmail.com or marilynlanes4s@gmail.com with 'OPT OUT' in the subject email field.

Individuals have the right to complain to the Information Commissioner office 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 a company (Support for Survivors Charity) must not hold onto data for any longer than is necessary. i.e**. , if Support for Survivors Charity were to keep a credit card detail several years after a contract has terminated.**

Support for Survivors are encouraged conduct regular reviews of the personal data they hold and securely destroy any information that is no longer relevant.

In other words - do not hoard. Only keep hold of old files if really needed or if you are required to by law.

Data Breaches

S4S 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 on all organization to report certain types of data breach to the ICO, and in some cases, to individuals.
- S4S only must 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 high risk to the rights and freedoms of individuals, we will also have to notify those concerned directly in most cases.

Examples

S4S suffers a breach that results in an accidental disclosure of one of our victims and survivors. There is most likely to be a significant impact on the affected victim and survivor because of the sensitivity of their personal data and their details become known to others. This is likely to result in a high risk to their rights and freedoms, so the victim and survivor must be informed of the breach.

S4S experiences a breach when one of workers accidently deletes a record of one of our victims and survivors. The victim and survivors' details are later re-created from a backup. This is unlikely to result in a high risk to the rights and freedoms of the victim and survivor. They do not need to be informed.

If we decide to notify individual, we will still need to notify the ICO unless we can demonstrate that the breach is unlikely to result in a risk to 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 high 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 explain the following.**

1. **GIVE the name and contact details of our data protection officer**
2. **Contact – as highlighted in red above**
3. **Description of the likely 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:-

S4S 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 Charities compliance with our notification duties under the GDPR.
As with any security incident, we must investigate whether or not 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 process, further training or other corrective steps.

Checklists

- ✓ SFS know how to recognise a personal data breach.
- ✓ SFS understand that a personal data breach is not only about loss or theft of personal data.
- ✓ SFS have prepared a response plan for addressing any personal data breaches that occur.
- ✓ SFS have allocated responsibility for managing breaches to a dedicated person or team.
- ✓ SFS work force know how to escalate a security incident to the appropriate person or team member in our Charity to determine whether a breach has occurred.
- ✓ SFS have in place a process to assess the likely risk to individuals because of a breach.
- ✓ SFS know and are aware who is the relevant supervisory authority for our processing activities.
- ✓ SFS have 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 have a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms.

GDPR created by Maxi 'Leigh (Founder Care Services Director

Signed: Maxi 'Leigh

Date: 5th April 2020