DATA PROTECTION PROTOCOL

Contents

1. Scope

1.1 The General Data Protection Regulations (GDPR) provide individuals with rights in relation to personal data held/processed by organisations. The GDPR also place obligations on organisations to have appropriate technical and organisational measures in place to ensure the integrity and confidentiality of personal information held/processed.

1.2 Suicide Bereavement UK holds and processes information about its staff, consultants, contractors, research participants and other stakeholders and third parties for various purposes including its obligations as a responsible and effective employer, in order to operate payroll and pension services and to comply with its obligations under the Data Protection Act to facilitate effective communication with those stakeholders. To comply with GDPR legislation information must be processed lawfully and fairly, collected for specified purposes, stored safely, be accurate and kept up to date as necessary and not disclosed to any unauthorised person or organisation.

1.3 Suicide Bereavement UK has a statutory obligation as a Data Controller/Processor to be responsible for and be able to demonstrate compliance with the legislation.

1.4 This policy defines the responsibilities of Suicide Bereavement UK and its employees, contractors and consultants and ensures that all are aware, not only of the requirements of data protection legislation on Suicide Bereavement UK itself, but also their individual responsibilities in this respect. A failure to comply with the provisions of GDPR may render Suicide Bereavement UK, or in certain circumstances the individuals involved, including relevant responsible Director(s), liable to criminal prosecution as well as giving rise to civil liabilities.

2. Responsibilities and Definitions

2.1 Suicide Bereavement UK Data Protection Officer is responsible for ensuring that statutory and regulatory obligations with respect to the GDPR are adhered to and for the provision of training, guidance and advice to ensure policy compliance by all employees, consultants and contractors. They are also the individual to whom all subject access requests and queries concerning personal data should be addressed.

2.2 The Information Commissioner's Office is the UK's independent authority set up to promote access to official information and to protect personal information.

2.3 Data Controller is the person or organisation who determines the purposes for which and the manner in which any personal data are, or are to be, processed. In our case Suicide Bereavement UK is the registered Data Controller.

2.4 Data Processor is any individual or company who records and/or processes personal data in any form on behalf of Suicide Bereavement UK.

2.5 Suicide Bereavement UK Directors are responsible for the promulgation of this policy and any associated guidance within their own business unit.

2.6 Permanent and temporary employees, contractors and consultants are responsible for incorporating this policy and its associated documents into their own working practices.

2.7 Data Processing in relation to this policy means:

- collection, recording, organisation, structuring, storage;
- carrying out any operation, or set of operations, on the information including:
  - organisation, adaptation or alteration of the information;
  - retrieval, consultation or use of the information;
  - disclosure of the information by transmission, dissemination or otherwise making available;
  - alignment, combination, blocking, erasure or destruction of the information.

2.8 Data Subject means any individual who is the subject of personal data, an employee, contractor, consultant, research participant, stakeholder or third party about whom Suicide Bereavement UK holds personal data.

2.9 Personal Data is defined as data which relate to an identified or identifiable person (data subject). An identifiable person is one who can be identified directly or indirectly. In particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person:

- from those data, or;
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller;
- and includes expressions of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of that individual.

2.10 Special categories of data refers to personal data revealing: racial or ethnic origins; political opinions, religious or philosophical beliefs; trade-union membership, genetic data, biometric data, data concerning health; sex life.

2.11 Subject Access Request is a written request from an individual to access any personal data that Suicide Bereavement UK holds about him/her. He/She also has the right to request the correction of any such data that is found to be incorrect.

3. Policy

3.1 The GDPR provides that six principles be adhered to in the processing of personal data. This is achieved by Suicide Bereavement UK implementing appropriate rules and procedures. All employees, contractors and consultants are therefore responsible for ensuring that these rules and procedures are followed. The objectives of the rules and procedures are to ensure that the 6 principles will be complied with and that all personal data is:

- processed lawfully and fairly and in a transparent manner;
- collected for specified, explicit legitimate purposes and not further processed in a manner incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes;
- accurate and where necessary kept up-to-date;
- kept in a form which permits identification for no longer than is necessary for the specified purpose;
- kept secure subject to appropriate technical and organisational measures against unauthorised or unlawful processing, accidental loss or destruction.

3.2 Under the terms of the GDPR, processing of data includes any activity to do with the data involved. All employees or other individuals who have access to, or who utilise, personal data, have a responsibility to exercise care in the treatment of that data and to ensure that such information is not disclosed to any unauthorised third party. Examples of personal data could include address lists and contact details as well as individual files. Any processing of such information must be done in accordance with Suicide Bereavement UK rules and procedures.

3.3 Additionally, in order to comply with the first principle, at least one of the following conditions must also be met:

- the subject has given his/her explicit consent to the processing (such consent must be recorded);
- the processing is necessary for the performance of a contract with the subject;
- processing is required under a legal obligation;
- processing is necessary to protect the vital interests (essential for the life) of the subject or another person;
- processing is necessary for the performance of a task carried out in the public interest;
- processing is necessary to pursue the legitimate interests of the Data Controller or third parties (unless it could prejudice the interests of the subject or would constitute processing carried out by a public authority in the performance of their tasks).

3.4 Special Category (sensitive) Data

If the personal data is deemed to be sensitive by the criteria described in 2.10, then additional conditions apply to its processing. Essentially, the explicit consent of the individual will usually have to be obtained before the data is processed unless the data controller can prove the processing is based on one of the following criteria:

- Compliance with employment law and obligations;
- To protect vital interests (essential for the life) of the data subject;
- The data subject has deliberately made the information public;
- To comply with legal obligations (establishing or defending legal rights);
- Processing is necessary for the establishment, exercise or defence of legal claims;
- Processing is necessary for reasons of substantial public interest;
- Occupational medicine, provision of heath or social care or treatment;
- Public health;
- Scientific or historical research or statistical purposes.

If you cannot justify the processing and holding of sensitive data, for one of the above reasons you must reconsider whether you should be gathering or holding that data at all. If the data needs to be held you must then obtain the explicit written consent from the data subject to ensure compliance (records of consent must be maintained to cover the entirety of the time the data is held/processed).

If you do not have a lawful basis to justify holding/processing this category of data, you must remove the data from your records.

3.5 Access rights

Data subjects have the right to access personal data that Suicide Bereavement UK holds about them. Such a request is called a subject access request (SAR). In summary, requests must be:

- processed by the DPO or suitably trained deputy;
- confirmed that the data subjects are who they say they are and have a right of access to the information;
- checked to ensure that any third party data subject's rights are not overlooked;
- responded to without undue delay and in any event within one month of receipt;
- recorded accurately.

3.6 It is also possible that Suicide Bereavement UK may also receive request from a data subject to erase personal data, rectify inaccurate data, restrict/cease or not begin processing personal data. All such requests or notices must be referred to the DPO and responded to either by:

- agreeing to comply with the request; or
- giving the reasons why the request is regarded as unjustified, either wholly or in part.

3.7 Privacy Impact Assessments

Privacy impact assessments (PIAs) are a tool that you can use to identify and reduce the privacy risks of projects. A PIA can reduce the risks of harm to individuals through the misuse of their personal information. It can also help you to design more efficient and effective processes for handling personal data.

A PIA should be carried out whenever a “new” project/process involving the use of personal information is being considered/initiated, especially if this involves the use of technology or third party processors e.g. new IT systems or contractors conducting work involving the processing of personal data.

Suicide Bereavement UK DPO should be consulted. The PIA template should be used to capture the process.

4. Documentation

- Records of subject access requests (Retained for 5 years);
- Records of communications resulting in an action to cease processing personal data (Retained for 5 years).

5. Appendices

Appendix 1: Anonymisation and Pseudonymisation Policy

Appendix 2: Arranging travel &/or associates’ administration tasks

Appendix 3: Suicide Bereavement UK GDPR Data Protection Guidance

Appendix 4: Suicide Bereavement UK Privacy Notice for Research Participants

Appendix 1: Anonymisation and Pseudonymisation Policy

The General Data Protection Regulations (GDPR) and Data Protection Act 2018, require us to use the minimum personal data necessary for a purpose. Secondary uses of personal information must not breach our obligations of confidentiality and respect for private and family life. Anonymisation and pseudonymisation enables Suicide Bereavement UK to undertake secondary use of personal data in a safe, secure and legal way.

The purpose of this policy is to ensure a standardised approach to enable consistency, with regard to how and when to anonymise or pseudonymise information.

Definitions

Anonymisation is the process of removing, replacing and/or altering any identifiable information (identifiers) that can point to the person(s) it relates to. Anonymisation is a term for a variety of statistical and other techniques that depersonalise information about people, so that the specific data subjects cannot be identified, including via aggregation and pseudonymisation.

Pseudonymisation is the de-identification of individual level information by attaching a coded reference or pseudonym to each record. This allows the information to be associated with a particular individual without that individual being otherwise identified.

Personal Identifiable Information (PII) is any information that can identify an individual. This could be one piece of information, or a collection of information, for example a name, address and date of birth.

Primary use refers to the use for which the information was collected/supplied to Suicide Bereavement UK. This also includes relevant supporting administrative processes and audit/assurance. Primary use requires information at the person identifiable level.

Secondary use refers to the use of information about individuals for research purposes, audits, service management, commissioning, contract monitoring and reporting. When PII is used for secondary uses the information should, where appropriate be limited and de-identified, so that the secondary use process does not enable individuals to be identified.

Aggregation is an anonymisation technique in which information is only presented as totals, so that no information identifying individuals are shown. Small numbers in total are a risk here and may need to be omitted or ‘blurred’ through random addition and subtraction.

Re-identification or de-anonymisation is where anonymised information is turned back into personal information through the use of data matching or combining. Where anonymisation is being undertaken, the process must be designed to minimise the risk of re-identification.

Why Anonymise?

Anonymisation is undertaken to protect the privacy of individuals, whilst still making data available for statistical or analytical purposes. Personal data does have to be used directly where the intention is to inform decisions about particular individuals, or to provide services to them. Where this information is not needed at this level and for these purposes, however, it should be anonymised. The GDPR is concerned with ‘personal data’ which relates to living individuals who can be identified from such data. Anonymised data where the prospect of identifying individuals is remote is not seen as personal data.

When anonymising information, Suicide Bereavement UK must be sure that information is assessed and risks mitigated. This includes assessing whether other information is available, that is likely to facilitate re-identification of the anonymised information.

The GDPR states that personal information is information which relates to a living individual who can be identified from that information, or from those information and information which is in the possession of, or is likely to come into the possession of, the data controller. When assessing whether information has been anonymised effectively, it is necessary to consider whether other information is available that, in combination with the anonymised information, would result in a disclosure of personal information. This is most likely where the circumstances described by the combined information are unusual or where population sizes are small.

Issues to consider are as follows:

- What is the risk of a 'jigsaw attack', piecing different items of information together to create a more complete picture of someone? Does the information have characteristics which facilitate information linkage?
- What other 'linkable' information is easily available?
- What technical measures might be used to achieve re-identification?
- What re-identification vulnerabilities did the motivated intruder test reveal?
- How much weight should be given to individuals' personal knowledge?

Anonymisation / De-identification

Staff should only have access to the information that is necessary for the completion of the business activity they are involved in. This principle applies to the use of PII for secondary or non-direct purposes. Through de-identification, users are able to make use of individual information for a range of secondary purposes without having to access the identifiable information items.

The aim of de-identification or anonymisation is to obscure the identifiable information items within the person's records sufficiently that the risk of potential identification of the information subject is minimised to acceptable levels: this will provide effective anonymisation.

De-identification can be achieved via a range of techniques. Whether de-identification is achieved depends on the fit of the technique with the specific dataset.

Techniques include:

- Aggregation so that information is only viewed as totals;
- Removing person identifiers;
- Using identifier ranges, for example: age ranges instead of age, full or
- partial postcode or super output area instead of full address, age at activity
- event instead of date of birth;
- Using pseudonyms.

De-identified information that goes down to the level of the individual should still be used within a secure environment with staff access on a need to know basis.

Transferring Information

Appropriate data sharing agreements should be in place when information is to be transferred to or from another organisation. If the transfer of information is required for secondary use then a form of anonymised or pseudonymised information should be sent.

Is Consent Needed to Produce or Disclose Anonymised Information?

An individual's properly informed consent is needed for the publication of personal data. However, there are obvious problems in this approach particularly where an individual decides to withdraw consent. In reality, it may be impossible to remove the information from the public domain, so that the withdrawal of consent will have no effect. Publishing anonymised information rather than personal data is safer even where consent could be obtained for the disclosure of personal data.

The 'necessity' rules in the GDPR mean that it could be against the law for Suicide Bereavement UK to publish personal data where anonymised information could serve the same purpose. In the Information Commissioner's view, it is generally acceptable to anonymise personal data and to disclose it without the data subject's consent provided that:

- The anonymisation will be done effectively, with due regard to any privacy risk posed to individuals – a privacy impact assessment could be used here;
- The purpose for which the anonymisation takes place is legitimate and has received any necessary ethical approval;
- Neither the anonymisation process, nor the use of the anonymised information, will have any direct detrimental effect on any particular individual;
- The data controller's privacy policy/notice – or some other form of notification - explains the anonymisation process and its consequences for individuals;
- There is a system for taking individuals' objections to the anonymisation process or to the release of their anonymised information into account.

Personal Information and Spatial Information

Postcodes and other geographical information will constitute personal data in some circumstances under the GDPR. For example, information about a place or property is, in effect, also information about the individual associated with it. In other cases, it will not be personal data. The context of the related information and other variables, such as the number of households covered by a postcode, is the key. The more complete a postcode or the more precise a piece of geographical information, the more possible it becomes to analyse it or combine it with other information to disclose personal data.

Publication and Limited Disclosure

Suicide Bereavement UK must make a decision whether to publish even anonymised information. Publication decisions should be informed by the realistic scope to control the use to which information is put following its release.

Access control where anonymised information or, in some cases, personal data, are disclosed but only to particular recipients, with conditions attached to the disclosure. This is often used between groups of researchers. It is appropriate for handling anonymised information that is particularly sensitive in nature or where there is a significant risk of re-identification. The great advantage of this approach is that disclosure is controlled.

Further information

For further advice and examples of anonymisation through aggregation, pseudonymisation and other techniques please refer to the Information Commissioner's code of practice

Appendix 2: Arranging travel &/or associated administration tasks

Please read the Employees Privacy Notice which describes how we collect and use your personal data in accordance with the prevailing UK data protection legislation, including the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA).

Purpose of processing

Suicide Bereavement UK is permitted to disclose personal data and other necessary information to external third parties who make travel arrangements on behalf of the organisation.

Lawful basis for processing

The lawful basis for processing your personal data, including your date of birth, address, passport number etc. is:

- 'contract' 6(1)(b), for staff i.e. the processing is necessary in order comply with obligations under the employment contact that Suicide Bereavement UK has with you;
- 'public task' 6(1)(e) if the purpose of the travel is linked to Suicide Bereavement UK's functions/powers; or
- 'legitimate interests' 6(1)(f) if the purpose of travel is for a legitimate reason other than in performance of Suicide Bereavement UK's functions/powers as a public authority.

In circumstances where we are processing special category data, including data revealing your racial or ethnic origin, religious beliefs and health information we need to identify both a lawful basis (as above) and a special category condition for processing in compliance with data protection legislation. In this instance the relevant conditions are:

- 'employment' 9(2)(b) for Suicide Bereavement UK staff;
- 'occupational medicine' 9(2)(h) for Suicide Bereavement UK staff when travel is related to occupational health;
- 'explicit consent' 9(2)(a). In this instance please complete the attached form. Unfortunately, failure to provide explicit consent in the limited number of circumstances where it is required may mean that Suicide Bereavement UK is unable to arrange travel on your behalf.

Please note, you have a number of rights in relation to your data. If you want to exercise any of these rights then you can do so by contacting the Data Protection Officer, Suicide Bereavement UK.

Appendix 3: Suicide Bereavement UK GDPR Data Protection Guidance

Here are some questions and answers to reassure you on how we use your data.

WHAT INFORMATION DO YOU COLLECT? We collect information that includes your name, address and contact details, as well as information about the organisation you work for/represent.

HOW DO YOU USE MY INFORMATION? We use your information to provide you with updates, guidance and services in relation to suicide bereavement. From time to time we'd like to send you information on updated or new products, services and special offers that are relevant to you and your organisation.

AND IS MY PERSONAL INFORMATION PROTECTED? All information that you give to us is kept secure, accurate and up to date. We do not sell your information to third parties for their own use.

AND HOW WILL YOU CONTACT ME? Normally we will contact you by post. However, if you would prefer to hear from us by email, please email us at admin@suicidebereavementuk.com with your full name. When you receive any marketing/ communication from us, you will have the ability to unsubscribe from our mailing list.

AND IF I DON'T WANT YOU TO CONTACT ME IN THE FUTURE? That's not a problem. Let us know and we will remove you from our mailing list.

WE do…

- Safely file away paperwork that contains customer information (name, address, telephone number, registration etc.) in a secure location;
- Always ensure paperwork is disposed of in confidential waste and not in the ordinary waste;
- When sending personal information relating to an employee or customer by email take extra care to ensure that the recipient's email address is correct.

We do NOT

- Leave paperwork containing personal information at any other location where it could be read by members of the public;
- Use a 'public access' computer for work purposes in relation to SBUK or download business data onto public devices;
- Write personal comments about a client or organisation in an email or on paperwork ;
- Leave our computer screens open/unlocked when we are not present.

Appendix 4: Suicide Bereavement UK Privacy Notice for Research Participants

Research at SBUK

The Suicide Bereavement UK (SBUK) privacy notice for research must be read in conjunction with a Participant Information Sheet made available to you by the research study you are taking part in. This contains details about the personal information collected for the particular project that concerns you. The research team will provide you with a copy of the information sheet.

SBUK conducts research to the highest standards of research integrity to ensure it is beneficial and contributes to wider learning. Our research is in the public interest. As part of our commitment to research integrity, we follow the UK General Data Protection Regulation (UK GDPR) and the UK Data Protection Act 2018 (DPA).

We promise to respect the confidentiality and sensitivity of the personal information that you provide to us. We will tell you how we use your information, how we will keep it safe and who it will be shared with. We commit to keeping your personal information secure and will not use it to contact you for any other purpose unless you have agreed to this.

Research has a special status under UK data protection law. Research conducted by our staff is defined as making an original contribution to knowledge which is published in order to share knowledge.

We are usually the Data Controller for research studies. This means that we will decide how your personal information is created, collected, used, shared, archived and deleted (processed). When we do this we will ensure that we collect only what is necessary for the project and that you have agreed to this. If any other organisation will make decisions about your information, this will be made clear in the Participant Information Sheet provided to you.

Information about you

‘Personal data’ means any information which can identify you. It can include information such as your name, gender, date of birth, address/postcode or other information such as your opinions or thoughts. It can also include information which makes it possible to identify you, even if your name has been removed. We will only ever collect personal information that is appropriate and necessary for the specific research project being conducted. The specific information that we collect about you will be listed in the Participant Information Sheet given to you by the research team.

We may process some information about you that is considered to be ‘sensitive’ and this is called ‘special category’ personal data. This includes, but is not limited to, information such as your ethnicity, sexual orientation, gender identity, religious beliefs, details about your health or past criminal convictions. These types of personal information require additional protections, particularly in relation to sharing, which SBUK ensures are in place.

Under UK data protection law we must have special safeguards in place to help protect your rights and freedoms when using your personal information and these are:

- Policies and procedures that tell our staff how to collect and use your information safely;
- Training which ensures our staff understand the importance of data protection and how to protect your data;
- Security standards and technical measures that ensure your information is stored safely and securely;

- All research projects involving personal data are scrutinised and approved by a research ethics committee;
- Contracts with companies or individuals not associated with SBUK have confidentiality clauses to set out each party's responsibilities for protecting your information.

In addition to the above safeguards, the UK GDPR and the DPA also require us to meet the following standards when we conduct research with your personal information:

- The research will not cause damage or distress to someone (e.g., physical harm, financial loss or psychological pain);
- The research is not carried out in order to do or decide something in relation to an individual person or their care, unless the processing is for medical research approved by a research ethics committee;
- The Data Controller has technical and organisational safeguards in place (e.g., appropriate staff training and security measures).

Legal provisions

Data protection law requires us to have a valid legal reason to process and use personal data about you. This is often called 'legal basis'. UK GDPR requires us to be explicit with you about the legal basis upon which we rely in order to process information about you.

For research, the legal reason is that 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller' (Article 6 of the UK GDPR).

For sensitive information the legal reason is 'the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes… which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject' (Article 9 of the UK GDPR).

When research involves criminal convictions, the legal reason is listed in Schedule 1 of the DPA which requires that special safeguards are in place.

Where we need to rely on a different legal reason, such as consent, this will be listed in the Participant Information Sheet provided to you.

We may also use your personal information for additional research purposes, such as other analyses or future projects on the same research topics. This is known as secondary use or purpose. If this is the case you will be informed in the Participant Information Sheet.

If we want to do this it will be explained to you in the Participant Information Sheet and we will ensure that your information will not be used in ways which might have a direct impact on you (such as damage or distress) or will lead to decisions being made about you.

Sharing your information

Your personal information will be kept confidential at all times and researchers are asked to de-identify (anonymise) it, pseudonymise (remove any information which can identify you such as your name and replace this with a unique code or key) it, or delete it as soon as possible. However, in some cases it may not be possible to de-identify your information as it

is necessary in order to achieve the aims of the research. If this is the case you will be informed in the Participant Information Sheet.

Your personal information as well as any de-identified information will only be shared with members of the research team in order to conduct the project. If they need to share your information with anyone else, you will be told who they are and why this is the case in the Participant Information Sheet.

We also sometimes use products or services provided by third parties to conduct research activities or share research data such as Dropbox for Business, Microsoft Teams, Zoom or other communication tools. These third parties are known as data processors and when we use them we have agreements in place to ensure your information is kept safe. This does not always mean that they access your information but if they do this will be outlined in the Participant Information Sheet. As Data Controller, we will always carry out due diligence in respect of the use of third parties in order to keep your information safe throughout the research.

Your rights

By law you have rights in relation to the personal information we hold about you. These include the right to:

- See the information/receive a copy of the information;
- Correct any inaccurate information;
- Have any information deleted;
- Limit or raise concerns about our processing of the information;
- Move your information;
- Request human intervention when automatic decision making or profiling is carried out. You will be informed if either of the above applies to your personal information.

These rights only apply to your information before it is anonymised as once this happens we can no longer identify your specific information. Sometimes your rights may be limited if it would prevent or delay the research. If this happens you will be informed by the research team but you still have rights to complain to our Data Protection Officer and if you are still not satisfied you also have the right to complain about this to the Information Commissioner.

If you have any questions about how your personal information is used or wish to exercise any of your rights, please contact:

The Data Protection Officer, Suicide Bereavement UK, 6-8 Taper Street, Ramsbottom, Lancashire BL0 9EX Email: paul.higham@suicidebereavementuk.com

If you are not happy with the way your information is being handled or with the response received from us, you have the right to lodge a complaint with the Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow, SK9 5AF (https://ico.org.uk/).