SP-UK

SUICIDE PREVENTION UK

Suicide Prevention UK

Data Protection and GDPR Policy

2024

Contents

Purpose

This policy sets out how Suicide Prevention UK complies with its data protection obligations and seeks to protect personal information relating to our staff and users of our service (referred to as service users).

Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

We are committed to complying with our data protection obligations and being concise, clear, and transparent about how we obtain and use personal information and how (and when) we delete it once it is no longer required.

Michael Everett (Founder and CEO), as our Data Protection Officer, is responsible for informing and advising Suicide Prevention UK and its staff on its data protection obligations and monitoring compliance with those obligations.

If you have any questions or comments about the content of this policy or if you need further information, you should contact the Data Protection Officer by emailing info@spuk.org.uk or by letter to Suicide Prevention UK, Suite 601, 179 Whiteladies Road,
Bristol, BS8 2AG.

Scope

This policy applies to the trustees, employees (full-time, part-time and casual), volunteers, contractors, and subcontractors of Suicide Prevention UK, who will be referred to as 'staff' throughout this policy.

This policy may be distributed to staff, service users, and other relevant third parties.

We will regularly review and update this policy following our data protection obligations. We will circulate any new or modified policy to staff and any other stakeholders when it is adopted.

For information, our Information Commissioner's Office registration reference is ZA776968.

Definitions

Criminal Records Information
Means personal information relating to criminal convictions, offences, allegations, proceedings, and related security measures, including Risk Level.

Data Breach
Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, personal information.

Data Subject
Means the individual to whom the personal information relates.

Personal Information
Sometimes known as 'personal data', means information relating to a natural individual who can be identified (directly or indirectly) from that information.

Processing Information
Means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it.

Pseudonymised
Is the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual.

Sensitive Personal Information
Means personal information about a natural individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

Processor
The UK GDPR defines a processor as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Processors act on behalf of the relevant controller and under their authority.

Controller
"Controller" means the natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the processing of personal data, where the EU or Member State laws determine the purposes and means of processing, the controller may be designated by those laws. Art.2(d) GDPR.

Data Protection Principles

Suicide Prevention UK will comply with the following data protection principles when processing personal information:

- We will process personal information lawfully, fairly and in a transparent manner;
- We will collect personal information for specified, explicit and legitimate purposes only and will not process it in a way that is incompatible with those legitimate purposes;
- We will only process the personal information that is adequate, relevant, and necessary for the relevant purposes;
- We will keep accurate and up-to-date personal information and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;
- We will keep personal information for no longer than is necessary and for the purposes for which the information was collected for processing; and
- We will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing and accidental loss, destruction, or damage.

The Basis for Processing Personal Information

Concerning any processing activity, we will, before the processing starts for the first time, and then regularly while it continues:

- Review the purposes of the processing activity and select the most appropriate lawful basis (or bases) for that processing, for example:
    - That the data subject has consented to the processing;
    - That the processing is necessary for the performance of a contract to which the data subject is a party;
    - To take steps at the request of the data subject before entering into a contract;
    - That the processing is necessary for compliance with a legal obligation to which Suicide Prevention UK is subject;
    - That the processing is necessary for the protection of the vital interests of the data subject or another natural person; or
    - That the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or

- That the processing is necessary for the legitimate interests of Suicide Prevention UK or a third party, except where the interests of fundamental rights and freedoms of the Data Subject override those interests.

Note: Except where the processing is based on consent, Suicide Prevention UK has satisfied itself that the processing is necessary for the relevant lawful basis (for example, that there is no other reasonable way to achieve that purpose).

- Document our decision as to which lawful basis applies to help demonstrate our compliance with the data protection principles.
- Include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s).
- Where sensitive personal information is processed, identify and document a lawful special condition for processing.
- Where criminal offence information is processed, identify and document a lawful condition for processing.
- Determine whether Suicide Prevention UK's legitimate interests are the most appropriate basis for lawful processing. To do this, we will:
    - Conduct a Legitimate Interest Assessment (LIA) and keep a record of it to ensure that we can justify our decision;
    - If the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);
    - Keep the LIA under review and repeat it if circumstances change; and
    - Include information about our legitimate interests in our relevant privacy notice(s).

Sensitive Personal Information

Suicide Prevention UK may need to process sensitive personal information. We will only process sensitive personal information if:

- We have a lawful basis for doing so set out above; for example, it is necessary for the performance of the employment contract to comply with Suicide Prevention UK's legal obligations for individuals or Suicide Prevention UK's legitimate interests; and
- One of the special conditions for processing sensitive personal information applies, for example:
    - The data subject has given explicit consent so that Suicide Prevention UK can provide its services.
    - The processing is necessary for exercising the employment law rights or obligations of Suicide Prevention UK or the data subject.
    - The processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent.
    - The processing relates to personal data, which are manifestly made public by the data subject.
    - The processing is necessary for the establishment, exercise, or defence of legal claims; or
    - The processing is necessary for reasons of substantial public interest.

Before processing any sensitive personal information, staff must inform the DPO of the proposed processing so that they may assess whether the processing complies with the criteria noted above.

Sensitive personal information will not be processed until:

- The assessment has been completed; and
- The individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Suicide Prevention UK will not carry out automated decision-making (including profiling) based on an individual's sensitive personal information.

Concerning sensitive personal information, Suicide Prevention UK will comply with the procedures set out to make sure that it complies with the data protection principles set out above.

During the recruitment process, we will ensure that (except where the law permits otherwise):

- During the shortlisting, interview and decision-making stages, no questions are asked relating to sensitive personal information, for example, race or ethnic origin, trade union membership or sexual orientation;
- If sensitive personal information is received, for example, the applicant provides it without being asked for it within their CV or during the interview, no record is kept of it, and any reference to it is immediately deleted or redacted;
- 'Right to work' checks are carried out before an offer of employment is made unconditionally and not during the earlier shortlisting, interview, or decision-making stages;
- During employment, we will process:
    - Health information to consider fitness to work, keep sickness absence records, and facilitate employment-related health and sickness benefits;
    - Sensitive personal information for equal opportunities monitoring and pay equality reporting. Where possible, this information will be anonymised.

Criminal Records Information: Staff

This type of data includes information about criminal allegations, convictions, and proceedings. It also includes information linked to security measures and restrictions, such as bail conditions, cautions, and restraining orders, and less obvious types of information, such as personal data relating to witnesses, victims of crime, and the absence of any criminal record or convictions, and details of allegations (proven and unproven). It may also include information about civil measures which may lead to a criminal conviction if not adhered to.

Generally, when we are processing special category or criminal convictions data, it is on the basis that the individual has given explicit consent to the processing.

Staff criminal records information will be processed following Suicide Prevention UK's legal requirements for DBS (Disclosure and Barring Service) checks on a case-by-case basis.

Where required by the Charity Commission, Trustees will be required to submit to DBS checks so that the Charity can ensure that its Trustees are not disqualified from this role by law.

Data Protection Impact Assessments (DPIAs)

Where the processing is likely to result in a high risk to an individual's data protection rights, either for internal Suicide Prevention UK operations or the execution of a contract, we will, before commencing the processing, carry out a DPIA to assess:

- Whether the processing is necessary and proportionate concerning its purpose.
- The risks to individuals; and
- What measures can be implemented to address those risks and protect personal information.
- Before any new form of technology is introduced, the manager responsible should contact the Data Protection Officer so that a DPIA can be carried out.
- During any DPIA, the Data Protection Officer will seek appropriate advice from the Trustees and other relevant stakeholders.

Documentation and Records

We will keep records of processing activities, including:

- The purposes of the processing;
- A description of the categories of individuals and categories of personal data;
- Categories of recipients of personal data;
- Where relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;
- Where possible, data retention schedules; and
- Where possible, a description of technical and organisational security measures.

As part of our record of processing activities, we document, or link to documentation, on:

- Information required for privacy notices.
- Records of consent.
- Controller-processor contracts.
- The location of personal information.
- Data Protection Impact Assessments.
- Records of data breaches.

If we process sensitive personal information or criminal records information, we will keep written records of:

- The relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;
- The lawful basis for our processing; and
- Whether we retain and erase the personal information following our policy document and, if not, the reasons for not following our policy.

We will regularly review the personal information we process and update our documentation accordingly. This may include:

- Carrying out information audits to determine what personal information Suicide Prevention UK holds.
- Distributing questionnaires and talking to staff across Suicide Prevention UK to get a more complete picture of our processing activities; and
- Reviewing our policies, procedures, contracts, and agreements to address areas such as retention, security, and data sharing.

We document our processing activities electronically so we can add, remove, and amend information easily.

General Controls in Place

There is a process of continual review to determine whether any changes in the organisation's registration are required as a result of changes in the nature of our work.

The details of Suicide Prevention UK are registered and kept up to date.

The notification to the Information Commissioner's Office is renewed annually.

Suicide Prevention UK maintains and updates the public data protection register, which will be reviewed regularly and at least annually.

Privacy Notices

Suicide Prevention UK will issue privacy notices from time to time, informing individuals about the personal information we collect and hold relating to them, how they can expect their personal information to be used and for what purposes.

We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

Individual Rights

Individuals have the following rights concerning their personal information:

- the right to access personal data held about them (the right of subject access);
- the right to be informed about how and why their data is used - and you must give them privacy information;
- the rights to have their data rectified, erased or restricted;
- the right to object;
- the right to portability of their data; and
- the right not to be subject to a decision based solely on automated processing.

Note: There are exemptions and restrictions that can, in some circumstances, be legitimately applied to exempt or qualify the right of individuals to exercise their rights. For example:

- If complying with an individual's request would jeopardise national security, defence, or public safety.
- If fulfilling the request would undermine the prevention, investigation, detection, or prosecution of criminal offences.
- In the interest of protecting public health, particularly in situations like controlling diseases or other health threats.
- If the processing of personal data is necessary for the establishment, exercise, or defence of legal claims.
- If fulfilling them would infringe upon the rights and freedoms of others, including trade secrets or intellectual property.

Individual Staff Obligations

Updating Personal Information

Individual staff members are responsible for helping Suicide Prevention UK keep their personal information up to date.

You must let us know if the information you have provided to us changes, for example, if you move to a new house or change your bank account.

Accessing Other's Data

You may have access to the personal information of other members of staff, current and ex-service users, partners and suppliers of Suicide Prevention UK in the course of your employment or engagement.

Therefore, Suicide Prevention UK expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out above.

If you have access to personal information, you must:

- Only access the personal information that you have authority to access, and only for authorised purposes.
- Only allow other staff to access personal information if they have appropriate authorisation.
- Only allow individuals who are not Suicide Prevention UK staff to access personal information if you have specific authority from the Data Protection Officer to do so.
- Keep personal information secure, for example, by complying with rules on computer access, password protection, secure file storage and destruction, etc.
- Not store personal information on personal devices.

You should contact the Data Protection Officer if you are concerned or suspect that one of the following has taken place (or is taking place or is likely to take place):

- Processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions being met;
- Any data breach as set out below;
    - Access to personal information without the proper authorisation;
    - Personal information not kept or deleted securely;
    - Removal of personal information, or devices containing personal information (or which can be used to access it), from Suicide Prevention UK's premises without appropriate security measures being in place;
- Any other breach of this policy or any of the data protection principles set out above.

Information Security

Suicide Prevention UK will use appropriate technical and organisational measures to secure personal information and protect against unauthorised or unlawful processing and accidental loss, destruction, or damage. These may include:

- Training staff on data protection and security;
- Ensuring that, where possible, personal information is pseudonymised or encrypted;
- Ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- Ensuring that in the event of a physical or technical incident, availability and access to personal information can be restored promptly; and
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In rare cases where Suicide Prevention UK uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

- The organisation may act only on the written instructions of Suicide Prevention UK ;
- Those processing the data are subject to a duty of confidence;
- Appropriate measures are taken to ensure the security of processing;
- Sub-contractors are only engaged with the prior consent of Suicide Prevention UK and under a written contract.
- The organisation will assist Suicide Prevention UK in providing subject access and allowing individuals to exercise their rights under the GDPR;
- The organisation will assist Suicide Prevention UK in meeting its GDPR obligations concerning the security of processing, the notification of data breaches and data protection impact assessments;
- The organisation will delete or return all personal information to Suicide Prevention UK as requested at the end of the contract; and
- Suicide Prevention UK will submit to audits and inspections, provide Suicide Prevention UK with whatever information it needs to ensure that they are both meeting their data protection obligations and tell Suicide Prevention UK immediately if it is asked to do something infringing on data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into or an existing agreement is altered, the relevant staff must seek approval of its terms from the Data Protection Officer.

Storage and Retention of Personal Information

Personal information (and sensitive personal information) will be kept securely following Suicide Prevention UK's principles below:

- Personal information (and sensitive personal information) should not be retained any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should follow Suicide Prevention UK's retention periods, which set out the relevant period or the criteria that should be used to determine the retention period. Where there is any uncertainty, staff should consult the Data Protection Officer.
- Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems, and any hard copies will be destroyed securely.

Data Breaches

A data breach may take many different forms, for example:

- Loss or theft of data or equipment on which personal information is stored;
- Unauthorised access to or use of personal information either by a member of staff or a third party;
- Loss of data resulting from an equipment or systems (including hardware and software) failure;
- Human error, such as accidental deletion or alteration of data;
- Unforeseen circumstances, such as a fire or flood;
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'Blagging' offences, where information is obtained by deceiving the organisation which holds it.

In the event of a Data Breach, Suicide Prevention UK will:

- Assesses the situation to determine the type and nature of the breach (sensitivity plus volume of personal data) and severity of consequences for individuals and make a record of the assessment.
- Immediately take such steps as are necessary to minimise the risk to data subjects and the organisation (for example, limiting further loss).

- Make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible, within 72 hours of becoming aware of it if it is likely to result in a risk to the rights and freedoms of individuals;
- Notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms, and notification is required by law.
- Take such steps as are necessary to ensure that similar breaches cannot happen again.

International Transfer of Data

Suicide Prevention UK does not intend to transfer personal information outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein and Norway) to other countries.

If this were to be required, it would be on the basis that that country, territory or organisation is designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards by way of standard data protection clauses.

Consequences of Failing to Comply

Suicide Prevention UK takes compliance with this policy very seriously. Failure to comply with the policy:

- Puts at risk the individuals whose personal information is being processed; and
- Carries the risk of significant civil and criminal sanctions for the individual and Suicide Prevention UK; and
- May, in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this policy, a staff member's failure to comply with any requirement may lead to disciplinary action under our procedures, which may result in dismissal for gross misconduct.

If a non-employee breaches this policy, their volunteering or working contract may be terminated immediately.

If you have any questions or concerns about this policy, do not hesitate to contact the Data Protection Officer.

Personal Data Processing

Internal Systems Used and Data Stored

The following core systems are used to store day-to-day operational information. Access is only provisioned to individuals with a legitimate need to know, and software access controls are managed internally.

The systems typically used are:

- Microsoft Office.
- The 1st Incident Reporting application (a cloud-based CRM with encrypted data in transmission; the data is stored securely in a Microsoft Azure Virtual Network).
- Member Mojo (a web-based cloud system).
- Halo Secure Vault (bodycam recordings).
- BT Cloud (Telephone recordings).
- Office Hard drive (CCTV recordings).

Physical Data Storage

Physical data (paper data storage) is secured when not in use and stored in locked filing cabinets and/or cupboards at our main premises.

Sharing of Data – Staff/Service Users

Staff and service user data are only shared when required with the following individuals and organisations:

- HMRC.
- Other Government Departments (if required to verify right to work).
- Pension Providers.
- Disclosure and Barring Service (if required).
- Welfare organisations and the authorities (Police, Ambulance Service, etc.)
- Local Authority departments such as Safeguarding Teams and Social Services.
- Payroll providers.
- Accountant/Bookkeeper.
- Other employers (where a reference for a team member is requested).

Staff Data Stored

This table details the specific data types stored, the reason the data is processed, the legal/legitimate reason, and the expected retention period.

Information Type
Staff Data
Data Stored
• Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses • Date of Birth • Place of Birth (from identity documents) • Sex • National Insurance Number • Bank account details, payroll records and tax status information • Work History • Criminal Records (as required) • Health data (if relevant to the role or the staff member's needs, for example, to implement reasonable adjustments, pay sick pay, etc.) • Emergency Contact Details • Salary/Wage • Annual Leave • Pension Information • Benefits Information • Start and leaving dates • Qualifications

• Copy of driving licence, passport, or other identity documents • Evidence of right to work in the UK/immigration status (as required) • Performance and Appraisal Information • Disciplinary and Grievance Information • Accident book, first aid records, injury at work and third-party accident information • Image and voice recordings (from CCTV and Bodycams) • Signature
Processing Reason
• Provision of employment or working obligations. • Fulfilment of contract.
Legal Interest/Legitimate Reason
• Legitimate reason for performing contract duties. • Consent is given by an individual at the initial stage (contract).
Retention Policy
2 years after the end of employment or working agreement.

Service User Data Stored

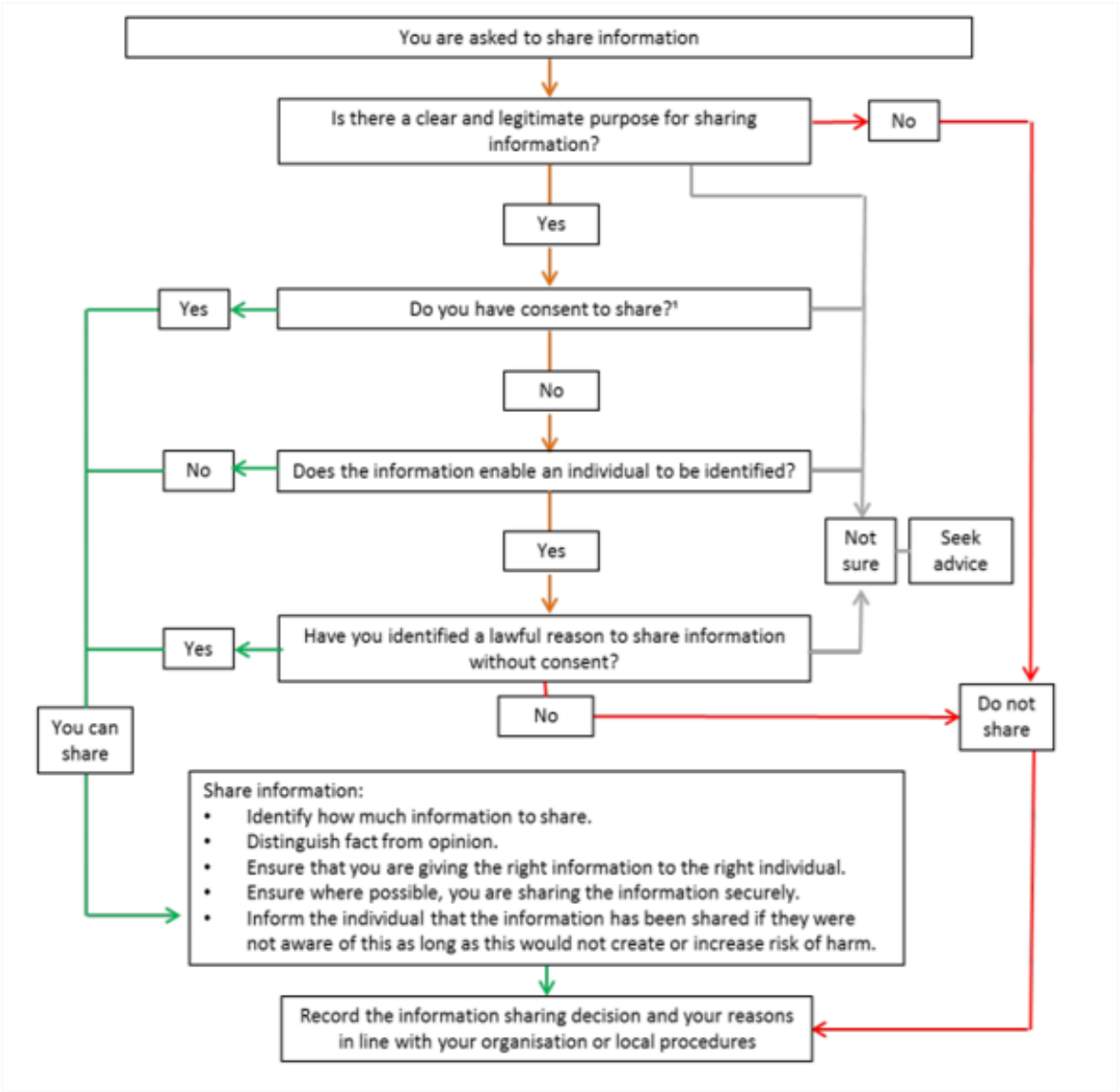
This table details the specific data types stored (if provided to us), the reason the data is processed, the legal/legitimate reason, and the expected retention period.

Information Type
Service User Data
Data Stored
• Personal contact details such as name, title, address, and contact number (of the caller or reporter) • Personal contact details such as name, title, address, and contact number (of the individual the caller is calling about or third party is making a report about) • Identification (e.g., Police identity cards) • Car registration number (if linked to an incident) • Location data • IP addresses (if using our website, see our Website Privacy Policy for further information) • Date of Birth/Age (of the individual the caller is calling about or third party is making a report about) • Health Data, including Disability Data (of the individual the caller is calling about or third party is making a report about) • Emergency Contact Details (of the individual the caller is calling about or third party is making a report about) • Agency Involvement (for example, healthcare providers or social workers of the individual the caller is calling about or the third party is making a report about). • Image and/or voice recordings (from CCTV, Bodycams and recorded calls) of the caller, reporter and/or individual the caller is calling about or the third party is making a report about. (See our Caller Privacy Policy for further information on call recordings and our CCTV and Bodycam Footage Policy for more information.)

Processing Reason
• Administration and Management of Suicide Prevention UK services. • Protection of our service users, staff, and the public.
Legal Interest/Legitimate Reason
• The processing is necessary for reasons of substantial public interest. • Vital Interests. • Explicit consent.
Retention Policy
5 years after the end of service provision (incident). 30 days following the recording of footage via CCTV or Bodycam (unless required for a longer period).

Data Sharing Process Flow

The diagram below represents a typical process flow for UK GDPR data sharing, the controls around data sharing and the actions that should be taken before sharing data.



Subject Access Requests

Introduction

Under GDPR legislation, Data Controllers shall provide the information outlined in Articles 13 & 14 to Data Subjects and Data Subjects may access, correct, delete, restrict processing of, and transfer their personal data, as well as object to automated decision-making based on their personal data.

SAR and Data Rights Procedure

Subject Access Requests (SAR) should come to the DPO email address in the first instance and be followed up with an acknowledgement letter/email.

All requests and their progress must be logged by the Data Protection Officer in a secure place with no external access.

SAR Timescales

All Subject Access Requests will be completed within 30 days unless defined as complex.

If the time will exceed 30 days, the requestor will be notified by return email to their request submitted to the DPO address.

SAR Fee's

Subject Access Requests coming directly from the data subject will be free. However, Suicide Prevention UK can charge a fee if requests become unfounded or excessive.

If requests are coming from another individual on behalf of a data subject, Suicide Prevention UK may charge a fee for data retrieval.

Monitoring and Reviewing

Suicide Prevention UK is committed to ensuring our policies are effective and up-to-date. To do this, we have a process for regularly monitoring and reviewing them.

The Trustees are responsible for this process and will review this policy at least once a year or more frequently if needed due to changes in laws or our practices.

Policy Date: October 2020

Review Date: April 2024

Next Review: April 2025

Dated and Signed by the Chair and Founder of Suicide Prevention UK:
