Breakthrough Data Protection Policy (GDPR)

Approved by Lead Organisation: November 2017
Reviewed March 2019
Reviewed November 2019
Next Review Date: November 2020

Introduction

The Partner organisations within the Breakthrough Programme need to collect and use certain types of information about the Data Subjects who come into contact with it in order to carry on our work. This personal information must be collected and dealt with appropriately– whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this in law. (General Data Protection Regulation (GDPR), Data Protection Act 2018).

This policy should be read in conjunction with the local Email and Internet Policy and the Safeguarding Policy.

Why this Policy exists

This Data Protection Policy ensures the programme:

- Complies with data protection law and follows good practice.
- Protects the rights of staff, customers and partners.
- Is open about how it stores and processes individual's data.
- Protects itself from the risks of a data breach.

1. Statement of policy

The Breakthrough Programme Partnership is fully committed to compliance with the requirements of the General Data Protection Regulation (GDPR), Data Protection Act 2018 and any successor legislation (together, the 'data protection legislation').
The partnership is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data and special category personal data.
The Breakthrough Programme will therefore follow procedures which aim to ensure that all employees and volunteers, and others who have access to any personal data held by or on behalf of the local office, are fully aware of and responsible for the handling of personal data in line with the data protection legislation.

In order to operate efficiently, the Breakthrough Programme partnership has to collect and use information about people with whom it works. These may include current, past and prospective clients; current, past and prospective employees; current, past and prospective volunteers; and our suppliers.

Data protection legislation and in particular Article 5 (1) of the GDPR requires that personal data shall be used in accordance with the following principles:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals;
b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."
Article 5 (2) of the GDPR requires that:
"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Lawful basis for processing personal data under the data protection legislation

The Breakthrough Programme primarily uses legitimate interest to process client personal data:

Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

The Programme may also process personal data under the following lawful bases:

Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

Lawful basis for processing special category personal data

The Programme Management Team processes special category personal data under the following lawful bases:

The GDPR defines special category data as:

• personal data revealing **racial or ethnic origin**;
• personal data revealing **political opinions**;
• personal data revealing **religious or philosophical beliefs**;
• personal data revealing **trade union membership**;
• **genetic data**;
• **biometric data** (where used for identification purposes);
• data concerning **health**;
• data concerning a person's **sex life**; and
• data concerning a person's **sexual orientation**.

Lawful bases used by the Breakthrough Programme

Explicit consent
Not-for-profit bodies
Archiving, research and statistics (with a basis in law)

Handling of personal data and special category personal data

The partnership will, through appropriate management and the use of appropriate controls adhere to the following in regards to our use of personal data and special category personal data;

● Provide up to data privacy notices to data subjects.
● Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with legal requirements.
● Ensure the quality and accuracy of information when collected or received and during its use.
● Apply checks to determine the length of time information is retained.
● Take appropriate technical and organisational security measures based on risks to data subjects.
● Not transfer outside the EEA without suitable safeguards.
● Ensure that any information incidents are reported to the Programme Management Team and where appropriate the data subject and the Information Commissioner's Office.
● Mitigate risks to the data subjects in the event of an information incident using an appropriate data breach policy.

● Ensure that the rights of our data subjects can be properly exercised.

These rights include:

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

In addition, we will ensure that:

● There is someone with specific responsibility for data protection in the organisation. The post responsible for data protection is Bill Basra, CEO Brancab (lead partner).
● Organisational information and in particular privacy risks are risk assessed, documented and controlled.
● Everyone managing and handling personal data and special category personal data understands that they are responsible for following good Information Governance / Assurance practice and for complying with the data protection legislation.
● Everyone managing and handling personal data and special category personal data is appropriately trained and supervised to do so.
● Queries about processing personal data and special category personal data are promptly and courteously dealt with within the requirements of the data protection legislation.
● Data sharing and processing is carried out under an appropriate written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.
All employees and volunteers are to be made fully aware of this policy and their duties and responsibilities under it. All employees and volunteers will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure.

Client management systems

Where the partner within the programme uses the relevant case management system provided by Citizens Advice, (currently Casebook) by doing so agrees to adhere to the data sharing agreement between the respective parties.
Citizens Advice and each individual local Citizens Advice are joint data controllers for the personal data and special category personal data within the Casebook application and therefore each have a joint responsibility to ensure compliance with data protection legislation.
Casebook is used to process information, personal data and special category personal data provided by clients in the course of seeking advice and guidance from the Citizens Advice service.

All information, personal data and special category personal data is to be regarded as being confidential between the individual and the Citizens
Advice service unless expressly indicated otherwise.
Data sharing is required so that both the client and Citizens Advice have flexibility in where, how and when clients receive the service and the need to only enter this client data once. The data protection legislation provides the legal framework under which personal data and special category personal data can be processed.
Data is shared to provide the service to clients, to refer clients to other organisations, for following up with the client for feedback, to enable
Citizens Advice to act on behalf of the client when authorised, to understand trends and carry out research to enable policy work. The data shared will always be the minimum necessary required to carry out the business purpose.
In all cases the relevant consent must be obtained, or alternative lawful basis determined, for any processing or sharing of client personal data and special category personal data.

Relationship with existing policies and supporting documentation

This policy has been formulated within the context of a range of policies such as those relating to IT security, confidentiality and information assurance.

Disclosure
The lead organisation may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows the partnership to disclose data (including sensitive data) without the data subject's consent.

These are:
1. Carrying out a legal duty or as authorised by the Secretary of State
2. Protecting vital interests of a Data Subject or other person
3. The Data Subject has already made the information public
4. Conducting any legal proceedings, obtaining legal advice or defending any legal rights
5. Monitoring for equal opportunities purposes – i.e. race, disability or religion
6. Providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.

Data collection
Informed consent is when

- A Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data
- and then gives their consent.

Partners will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, by completing a form, over a telephone, from a website or third party supplier..
When collecting data, Partners will ensure that the Data Subject:

- Clearly understands why the information is needed
- Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing
- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
- Has received sufficient information on why their data is needed and how it will be used

Data Storage
Information and records relating to service users will be stored securely and will only be accessible to authorised staff.

When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

It is the responsibility of all partners to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

Data access and accuracy
All Data Subjects have the right to access the information the programme holds about them. Partners will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition, partners will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection,
- Everyone processing personal information understands that they are contractually responsible for following good data protection practice,
- Everyone processing personal information is appropriately trained to do so,
- Everyone processing personal information is appropriately supervised,
- Anybody wanting to make enquiries about handling personal information knows what to do,
- It deals promptly and courteously with any enquiries about handling personal information,
- It describes clearly how it handles personal information,
- It will regularly review and audit the ways it hold, manage and use personal information
- It regularly assesses and evaluates its methods and performance in relation to handling personal information
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

In case of any queries or questions in relation to this policy please contact the Breakthrough Programme Management Team.

For general information on data protection please visit https://ico.org.uk/