



General Data Protection Regulations (GDPR) Policy

1. Introduction

The UK's Data Protection Act 1998 (DPA) and the EU's General Data Protection Regulation (GDPR) are both intended to regulate the processing of "personal data" by individuals and organisations.

Anyone recording, processing or obtaining information about individuals must ensure they are complying with these regulations.

The Brigitte Trust's policy on Data Protection is defined in this document and sets out specific requirements for processing and managing personal data.

The Brigitte Trust is registered as a "Data Controller" under the Data Protection Act.

1.1 Definitions

Data Protection Officer - For the purpose of this document the Data Protection Officer is the person charged with co-ordinating compliance under DPA and GDPR legislation. In practice The Brigitte Trust is not a large enough organisation to have one person dedicated to this task so the role may be shared by various people but the Charity Manager will take primary responsibility.

Data Controller - Under UK legislation there can only be one "Data Controller" for each registration (or notification) under the DPA. The Data Controller is therefore registered as The Brigitte Trust.

Data Subject - Any individual about whom data is stored or processed.

Personal Data – Information held by The Brigitte Trust about an individual (including clients, supporters, professionals, volunteers, trustees and employees).

Processing - is any activity that involves use of personal data, whether or not by automated means. It includes but is not limited to:

- (a) collecting;
- (b) recording;
- (c) organising;
- (d) structuring;
- (e) storing;
- (f) adapting or altering;
- (g) retrieving;
- (h) disclosing by transmission;
- (i) disseminating or otherwise making available;
- (j) alignment or combination;
- (k) restricting;

- (l) erasing; or
- (m) destruction of personal data.

Sensitive Personal Data (which is defined as “special categories of personal data” under the GDPR) - includes information about a person's:

- (a) racial or ethnic origin;
- (b) political opinions;
- (c) religious, philosophical or similar beliefs;
- (d) trade union membership;
- (e) physical or mental health or condition;
- (f) sexual life or orientation;
- (g) genetic data;
- (h) biometric data; and
- (i) such other categories of personal data as may be as “special designated categories of personal data” under the Legislation.

1.2 Responsibilities

The following sections describe responsibilities specifically in respect of Data Protection.

1.2.1 Brigitte Trust Management

Brigitte Trust Management (i.e. Charity Manager) is responsible for:

- implementing data security controls and policies that are appropriate for ensuring compliance with all relevant UK and EU regulations;
- maintaining the Brigitte Trust’s registration with the Information Commissioner’s Office;
- ensuring that all employees and volunteers are made aware of their obligations to comply with the policies set out in this document and other related documents.

1.2.2 All Staff, Trustees & Volunteers

All staff, trustees and volunteers are responsible for:

- complying with the policies set out in this document and the Brigitte Trust E-Safety and Security Policy;
- ensuring the confidentiality of all personal data that they have access to;
- ensuring appropriate consent is granted and recorded, as set out in this document and in any procedures manual issued to them, whenever personal data is collected or utilised;
- reporting any known or possible data breach **immediately** to the Charity Manager

General Principles of Policy

GDPR and DPA regulations cover everyone about whom you keep personal data. This includes:

- Clients/Service users: People who receive BT emotional and practical support, clients and family members.
- Employees: Individuals employed by the Brigitte Trust
- Volunteers: Individuals who provide their time and skills for free and include those who provide emotional and practical support to clients, trustee's, patrons, IT persons, research support and profile raising.
- Members of BT: Individuals who pay a yearly subscription, have voter's rights at BT's AGM and receive newsletters from the Brigitte Trust.
- Supporters- Individuals who support BT promotional events.
- Donors: Individuals who provide donations and/or legacies to BT

It is the intention of this policy that The Brigitte Trust will comply with the requirements of both the GDPR and the DPA.

Together, the GDPR and the DPA regulate the “processing” of any information relating to individuals. In the case of Brigitte Trust this will include:-

- any personal and sensitive information collected and processed in the ordinary course of providing our service – this will include data about clients; referrers, volunteers, professional contacts, trustees and supporters
- any personal and sensitive information collected and processed in relation to staff / employees;

The legislation:

- requires organisations to register with the Office of the Information Commissioner if they process personal data
- governs the processing of personal data including 'personal sensitive data'
- allows anyone, about whom you hold personal data, to request to see the personal data held on them; to have that data rectified if it is incorrect or incomplete; in some circumstances to have the data erased and to restrict how that data is processed or used.

Article 5 of the GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- 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;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 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;
- 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
- 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. NB 2 Please see Data Protection Framework for timescales.

Article 5(2) requires that:

- the controller shall be responsible for, and be able to demonstrate, compliance with the principles.

The Brigitte Trust Policy Section

1.3 Registration under the UK Data Protection Act

The Brigitte Trust Charity Manager (or whoever is appointed by them to act on their behalf) is responsible for maintaining The Brigitte Trust's registration under the Data Protection Act and ensuring it is complete and up to date.

1.4 Security

The Brigitte Trust Charity Manager (or whoever is appointed by them to act on their behalf) must ensure appropriate security measures are in place to safeguard personal data.

The primary data storage systems utilised by The Brigitte Trust are provided by third parties – Dizions Ltd (Charitylog) and Microsoft Corporation (Office 365) who we have contracts with. Where personal data is processed by a third party, the Charity Manager must ensure that appropriate security arrangements are being followed by the third party. The Charity Manager should therefore only appoint processors who can provide "sufficient guarantees" that the requirements of the GDPR will be met and the rights of data subjects protected. This may be in the form of a written agreement, a letter or e-mail from the third party confirming how data is secured or by undertaking an assessment of the third party as a suitable partner to act in such a role (or a combination of these approaches).

All such decisions CONTACTS to utilise a third party should be documented (Please see BT Data retention Framework for more details).

The CHARITY MANAGER must also ensure that any data held on Brigitte Trust laptops or desktop computers is adequately secured and staff are aware of their responsibilities in this regard. Specific guidelines are included in The Brigitte Trust E-Safety and Security Policy document.

1.5 Data Processing

The Brigitte Trust has 4 main purposes for processing personal data:

- **Provision of The Brigitte Trust support service for clients.**
Client data is used by volunteers, SCO, Supervisors and Management to ensure that the service provided to clients is appropriate and meets the standards required by the Trust.
- **Fundraising for and Marketing of the service offered by The Brigitte Trust.**
Contact details of supporters, volunteers, health professionals, clients and their relatives may be contacted for the purpose of explaining the service offered by the Trust and to support fundraising initiatives.
- **Provision of statistical data.**
Statistical data (which does not normally include personal identifiers) is used to support the management of the service and to support funding from other organisations (such as Macmillan Cancer Support, local councils, charitable trusts etc.) that may provide funding for The Brigitte Trust.
- **HR support and staff payroll.**
Staff data is used to support the HR function of The Brigitte Trust.

There are six available lawful bases for processing. Of these there are three that are most relevant to The Brigitte Trust.

1.5.1 Consent

This will be the usual lawful basis for processing client and volunteer data to enable the:

- provision of The Brigitte Trust service;
- collation of statistical data;
- the distribution of fundraising and other direct marketing materials.

When fundraising and direct marketing materials are distributed the recipients will be given the opportunity to “opt out” of future mailings.

1.5.2 Contract

This will be the usual lawful basis for processing staff data for the:

- payment of salaries and related tasks.

1.5.3 Legitimate Interests

This will be the usual lawful basis for processing data relating to all types of related parties for the:

- the distribution of newsletters to professionals
- the distribution of newsletters to beneficiaries, supporters and members.

When newsletters are distributed the recipients will be given the opportunity to “opt out” of future mailings.

1.6 Right to be Informed / Privacy Notices

1.6.1 Consent

As a general principal, The Brigitte Trust will obtain consent whenever it collects personal data directly from the data subject.

When data are collected from a third party (such as referrers) the data subject will be informed of the categories of personal data received and this will be done within a reasonable period of having obtained the data (normally within one month). The data subject will be asked to consent to the data being recorded by The Brigitte Trust.

Personally Collected Consent

In all cases where consent is requested personally, the data subject will be asked to sign a “Privacy Notice” which includes:

- Why the data is being collected.
- How it will be used, with an opt-in / opt-out option for each purpose.
- Who it will be shared with (if required).
- The right to opt-out at any time.

Impersonally Collected Consent

Where data is collected via an on-line form, e.g. via the Brigitte Trust website, the Brigitte Trust will include a “tick box” to indicate consent and access to an appropriate “Privacy Notice” that can be accessed by the data subject.

1.6.2 Disclosure

If disclosure to another recipient is envisaged (for example if a client is being signposted to another organisation), the data subject must give consent before the data are disclosed.

1.7 Subject Access Rights

Under the GDPR, individuals have the right to obtain access to their personal data so that they are aware of and can verify the lawfulness of the processing

In normal circumstances The Brigitte Trust will provide a copy of the data held at the earliest possible time but no later than within 1 month of receiving the written request. In line with the requirements of the GDPR there will normally be no charge made for providing the data.

Persons making an enquiry or requesting access to their data will be provided with a subject access request form (see Appendix 1). This form will:

- Request the information required to locate the data requested e.g.- an individual should provide their full name; the nature of their relationship with The Brigitte Trust (e.g. ex-member of staff); the approximate dates of that relationship; any other information which may assist in locating the data.
- Request Proof of Identity to be provided.
- Indicate that the response will be provided promptly and in any event within 30 days of receiving the required information.

1.8 Right to Rectification / Erasure / Restrict Processing / Object

1.8.1 Rectification

If The Brigitte Trust is advised by any data subject that the data held about them is incorrect it will be corrected at the earliest opportunity and no later than 1 month after receiving the notification. If the data has been disclosed to any third party, then that third party will also be informed of the correction.

1.8.2 Erasure

If The Brigitte Trust is advised by any data subject that the data held about them should be erased, it will be erased or anonymised at the earliest opportunity and no later than 1 month after receiving the notification. If the data has been disclosed to any third party, then that third party will also be informed of the requirement for it to be erased.

Note: In some circumstances this could result in The Brigitte Trust no longer being able to provide its service to a client. In such circumstances the client will be advised accordingly.

1.8.3 Restrict Processing / Object

If The Brigitte Trust is advised by any data subject that the data held about them should no longer be used for a specific purpose, this will be recorded on their record and that purpose will be discontinued. This is most likely to occur in relation to direct marketing or similar processes.

1.9 Transfer of Personal Data Overseas

The Brigitte Trust does will not transfer personal data overseas.

1.10 Data Breaches

The GDPR introduces a duty on all organisations to report certain types of data breach to “the relevant supervisory authority”. In some cases, organisations will also have to report certain types of data breach to the individuals affected.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

For example The Brigitte Trust could be responsible for a personal data breach if a client’s record containing personal health data is inappropriately accessed.

A data breach only has to be notified to the relevant supervisory authority where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

This has to be assessed on a case by case basis. For example, The Brigitte Trust would need to notify the relevant supervisory authority about a loss of client details where the breach leaves individuals open to identity theft or significant loss of confidentiality. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases.

At the time of writing the “relevant supervisory authority” for the Brigitte Trust will be The Charity Commission for England and Wales.

It may also be necessary to report the breach to the Information Commissioner’s Office. Their advice should be sought accordingly.

2. Use of Computer Systems and Manual Systems

2.1 Brigitte Trust E-Safety and Security Policy

This policy document describes the good practice guidance and rules which staff and volunteers working for the organisation should follow when using IT equipment and systems, accessing the internet and using e-mail and other electronic methods of communication. It covers working in the office, working whilst in the community and remotely accessing Brigitte Trust's files and / or e-mail.

2.2 Charitylog

The Charitylog system is the main data processing system utilised by The Brigitte Trust and holds personal data relating to individuals with various relationships to the organisation – in particular client data.

Particular care must be taken when extracting personal data from Charitylog to ensure that it is:

- stored safely;
- deleted when no longer required;
- not transferred outside of the organisation without appropriate consent.

If data is transferred by email to volunteers or other members of the organisation, for example in the form of a spreadsheet or word-processing document, it should be secured by using a password to lock the document and the password should be passed on in a separate email.

Data in Charitylog is used to produce vital statistics used by the Trust. Charitylog has a feature that enables data to be "anonymised". Therefore if a person requests that their data be erased this feature will be used to enable the Trust to continue to produce statistics but without identifying the specific individual.

2.3 Microsoft Office 365

Office 365 is a cloud based file storage system used by the Trust as the main depository for all general files (documents, spreadsheets photographs etc.) It is therefore possible that personal data may be held and processed using data held in this system (this is particularly possible in the case of spreadsheet based data).

Therefore the same level of care must be taken with data in Office 365 as that held within Charitylog namely to ensure that it is:

- stored safely;
- deleted when no longer required;
- not transferred outside of the organisation without appropriate consent.

The same approach as for Charitylog must be adopted when transferring personal data files via email between members of the organisation.

2.4 Website

The Brigitte Trust public website (www.brigitte-trust.org) is not used to process data however it does contain some personal data and is used to collect some personal data.

Therefore the website will:-

- incorporate a suitable “Privacy Notice” document that can be accessed by any user;
- include a pointer to the “Privacy Notice” in any on-line forms that collect personal data;
- include “opt-in / opt-out” and / or “consent” tick boxes as appropriate on on-line forms that collect personal data;
- include an appropriate “Privacy Notice” on any downloadable forms that may be used collect data off-line.

2.5 E-mail Systems

Email is not a totally secure medium and therefore care must be used if transmitting personal or confidential information. Attachments containing confidential information must be protected with a password which is passed to the recipient in a separate email or verbally.

Date reviewed	January 2020
Date to be reviewed	December 2022
Date approved	February2020

3. **Appendix 1 – Data Subject Access Request Form**

	<p>The Brigitte Trust Personal Data Access Request</p>
<p>Full Name:</p>	
<p>Address</p>	
<p>Relationship to The Brigitte Trust</p>	<p>Ex Staff / Volunteer / Client / Other <i>(Delete as appropriate)</i></p>
<p>Approximate Dates of Relationship</p>	<p>From: To:</p>
<p>Please describe the nature of the data requested</p>	

Please provide one form of identification showing your current address, from the following list:

1. Photocopy of Passport
2. Photocopy of Driving Licence
3. Photocopy of Utility Bill

Signed: _____ Date: _____