General Data Protection Regulation Policy

Date Reviewed: 9 November 2021
Next Review: 1 June 2022

Policy Summary

This policy reflects the Cherie Blair Foundation for Women's commitment to the Data Protection Act 2018, which is the UK's implementation of the General Data Protection Regulation (GDPR). Everyone responsible for using personal data must follow strict rules called 'data protection principles'. They must make sure the information is: used fairly, lawfully, and transparently.

This policy outlines the Foundation's approach when handling data and the subsequent roles and responsibilities.

Contents

Organisational Accountability:

Data Protection Officer (DPO) and other roles

The Trustees for The Cherie Blair Foundation for Women (the Foundation) is ultimately accountable for strategic approach to data protection.

Based on an assessment of the criteria outlined in the GDPR it has been concluded that the Foundation is not required to appoint a statutory Data Protection Officer (DPO). It has voluntarily chosen to appoint a DPO.

The DPO is Director of Finance and Corporate Services. The DPO is responsible for providing data protection oversight and expertise to the organisation as a whole.

The DPO has operational responsibility for CBFW's good practice and will be accountable for maintaining the Data Controller notification and Records of Processing Activity

All staff, including volunteers, contractors and temporary workers, are required to understand and comply with CBFW's data protection standards and procedures.

We will meet our accountability obligations by adopting the approach to monitoring performance and risk outlined under the heading *Performance and Risk*.

Data Protection Policy and ICO Data Protection Fee/Registration

The Foundation will maintain a Data Protection Policy (DPP).

The Foundation will pay the required data protection fee and be registered with the Information Commissioner's Office (ICO) with the following reference: ZA338176.
It is the responsibility of the DPO to maintain the ICO registration.

As a United Kingdom based charity, the Foundation is committed to the GDPR legislation which is retained in domestic law as the UK General Data Protection Regulation (UK GDPR). This legislation sits alongside an amended version of the Data Protection Act 2018.

The UK GDPR also applies to controllers and processors based outside the UK if their processing activities relate to:

- offering goods or services to individuals in the UK; or
- monitoring the behaviour of individuals taking place in the UK.

Training and awareness

The Foundation will ensure staff receive data protection training and awareness by providing:

- Mandatory elearning, and
- Annual updates to training

The Foundation will ensure volunteers who handle personal data receive data protection training and awareness by:

- Mandatory elearning.

Performance monitoring

The Foundation's approach to monitoring compliance is as follows:

- Breaches
- Procurement
- New projects (DPIAs)
- Rights Requests / Objections (see *Transparency Section*)
- New data collection activities (see *Transparency Section*)

Data Protection risk

The Foundation has documented its tolerance of risk (e.g. potential impacts) to the organisation and for individuals with regards the handling of personal data as indicated in the GDPR Risk Register and organisational Risk Register.

Monitoring of data protection risk is overseen by the **DPO**. Risks can be escalated to issues when the DPO considers the risk as become an active issue for the Foundation.

Data Protection issues

The Foundation documents compliance issues alongside the Risk Register. Strategic monitoring of data protection issues is overseen by the **DPO** and reported to **Trustees** on an annual basis and/or when urgent issues arise.

What is considered Personal Data?

personal data is any piece of information that someone can use to identify, with some degree of accuracy, a living person. This includes information pertaining to:

- A name and surname
- A home address
- An email address
- An identification card number
- Location data
- An Internet Protocol (IP) address
- The advertising identifier of your phone

Definition under the Data Protection Act 2018 (DPA): data which relate to a living individual who can be identified:

- (a) from those data; or
- (b) 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 any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Definition under the GDPR: any information relating to an identified or identifiable natural person.

What is considered Sensitive Data?

The DPA defines sensitive personal data as a specific set of "special categories" that must be treated with extra security. This includes information pertaining to:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data; and
- Biometric data (where processed to uniquely identify someone).

Definition under the GDPR: data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Legal Basis

The lawful bases for processing are set out in Article 6 of the UK GDPR:

A) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
B) **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.
C) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
D) **Vital interests:** the processing is necessary to protect someone's life.
E) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
F) **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 Foundation operates largely under Legitimate Interest. In particluar;

Corporate Services Department:

We use **Contract** and **Consent** for the following reasons:

1) We recruit and hire staff to work and volunteer for the Foundation
2) We sign and engage with contractors, suppliers, and partners in which a legal contract is obligatory

This department also operates largely within the sphere of **Legal Obligation** and **Public Task.**

Private information relating to individuals is stored in a private folder (Human Resources – CEO Only) on the W-Drive that only the four members of Corporate Services (including the CEO) can access.

Information relating to business relationships and stakeholders is stored in a private folder (Finance - Confidential) on the W-Drive that only the four members of Corporate Services (including the CEO) can access.

External Affairs Department:

We use **Legitimate Interest** and **Consent** for the following reasons:

1) To collect information about programme participants for the communication of the impact of our work. This can be both personal data, quotes and photographs.
2) To ensure that we protect the personal and business interests of the women we work with.
3) In order to fulfil our legal obligations, both in relation to the rights of the women we work with, but also the need for statistical analysis for the Annual Report etc.
4) We have contractual obligations with our funding partners which require External Affairs engagement.

The External Affairs department store the information in the following locations:
- Dropbox (stored for 5 years until being officially archived, but not deleted)
- In the W-Drive (External Affairs folders)

The External Affairs team also use a consent form with details when, how and why the information or photographs are being used, and at what point it will cease to be used by the Foundation. New consent forms are being drafted for completion at the end of 2021. These consent forms will also be produced in the language applicable to the country or programme to ensure informed consent with complete understanding.

Partnerships Department:

We use **Legitimate Interest** for the following reasons:

1) Any persons or companies who funds a campaign or donates money is recorded for business and legal purposes. This information is stored on Raiser's Edge (CRM) and Quickbooks.
2) To monitor and keep abreast of information relating to these stakeholders in regard to how they interact and engage with the Foundation.
3) For tracking and monitoring prospects who have indicated an interest or financial engagement with the Foundation or our Founder.

The Partnerships team mainly keeps information that is found online in the public domain. They also use **Contract** and **Legal Obligation** when working with and contracting partners and donors for the Foundation.

All information relevant to personal and/or business data is saved on Raiser's Edge (RE) and the appropriate W-Drive folders which are managed and maintained by the department.

Programmes Department:

We use **Legitimate Interest** for the following reasons:

1) Understand the profile of the women entrepreneurs
2) Understand the business sectors they are operating in
3) Understand the impact of our programmes
4) Ability to follow up for evaluation purposes/cases studies/et cetera.
5) By applying to be a participant of our programmes we require information relating to their businesses in order to effectively support and guide them through the programme.

Information relating to the Mentoring department is stored on Mentorloop and Survey Monkey. Access to these platforms is maintained and monitored by a manager within the Mentoring team. All members of the Mentoring team can access Mentorloop due to the nature of the work they are required to do.

Survey Monkey can only be accessed by one staff member in the Mentoring team and one staff member in the Entrepreneurship team. This is also due to the security functions required by Survey Monkey.

The Programmes department keep personal data and information for up to two years before it is anonymised. This information is saved on the W-Drive in the Mentoring folders and Monitoring, Evaluation and Learning folders and access is restricted.

The Programme department also use **Contract** and **Legal Obligation** when working with their partners and women entrepreneurs.

Personal and Sensitive Data Breaches:

Managing Personal Data Breaches

Staff are made aware of the process for raising an actual or suspected data protection breach:

- Annual training for all staff, posters in office, PowerPoint presentations

The following procedure is followed for handling data protection breaches:

- Personal Data Breach Procedure

It is the responsibility of staff to follow the Personal Data Breach Procedure, and by doing so they:

1) Contact their line manager, department Director and DPO (Director of Corp. Services and Finance). The DPO is now responsible for monitoring the 48 hour legal window in which reporting may be required depending on the nature of the breach
2) Staff member reporting the breach is to complete CBFW Internal GDPR Breach Report Form
3) Email form as soon as possible to the DPO, line manager, and department Director
4) Follow up email to DPO with a phone call
5) The staff member and the DPO must complete, the Personal Data Breaches and Assessment Log to the best of the reporter's ability.
6) The DPO ensures that the Personal Data Breach Log is maintained. The following role is responsible for it: Director of Corporate Services and Finance
7) The DPO must now follow the Personal Data Breach Procedure to determine and assess whether or not the breach meets the GDPR criteria for notification to the ICO within the 48h window

A log of breaches is maintained, and reported on as part of our performance and risk monitoring:

- Data Breach Log and Assessment Tool

Notifying the ICO / informing individuals of a personal data breach

The following process is used to assess incidents: assessment criteria defined in breach procedure.

The decision on whether to inform individuals is made by the DPO with consideration of the impact on the rights and freedoms of Data Subjects guiding whether to inform them.

The trustees and CEO may also be involved in making this decision.

Record of Processing Activities (ROPA) (to be completed summer 2021)

ROPA & Appropriate Policy Document

We will maintain a ROPA. As a minimum, this

- contains core and high-risk activities to the Data Subject;
- maps core and high-risk data journeys to the Data Subject;
- includes (or contain reference) to any Legitimate Interests Assessment required for core and high-risk activities that rely on the Legitimate Interests lawful basis;
- is updated each time a new purpose of processing is identified, and a review of the lawful basis for that Processing will be carried out; and
- is reviewed for accuracy and currency by the DPO every year.

Transfers of Personal Data outside the UK

The requirement for Personal Data to be transferred outside the UK will depend on the purposes of processing, which is documented in our ROPA. The condition for transfer will also be determined by the purpose.

Transfers to high human rights risk destinations are identified (by contractors and partners); suitable conditions for transfer are identified and recorded in our ROPA.

Working with suppliers and partners

Procurement and engagement

In order to ensure the Foundation meets its obligations to manage and protect Personal Data

- due diligence must be undertaken of all suppliers and partners (including consultants) and partners who will handle Personal Data on behalf of, or in partnership with the Foundation;
- no contract or Data Sharing Agreement will be entered into without sufficient due diligence and the appropriate clauses / Agreement or terms in place, and
- we use Non-Disclosure Agreements when engaging consultants or contractors (e.g. individuals, sole traders).

When seeking to engage new suppliers or partners, we will record who has the authority to agree that a contract / Agreement meets the requirement standards – e.g staff must consult **DPO** and obtain their agreement before any contract or DSA is signed.

A log of all external relationships is maintained. This log is maintained in our CRM system, Raiser's Edge under the constituency code 'Data Processor.'

- Includes details of the nature of relationship arrangements
- Includes details of any high-risk relationships - the DPIA Screening - Questions.docx form will be the tool used to decide this;
- Is reported on as part of our performance and risk monitoring

Relationship records

Copies of contracts and agreements for high-risk relationships are monitored by each Team and stored on our CRM system. This has been agreed with our Director of Corporate Services.

Integrating Data Protection

Data Protection by Design and Default

Data protection by design and default ("DPbD2") will be embedded into our change and project management processes by the end of 2022.

Data Protection Impact Assessment (DPIA)

An assessment of new processing activities will be undertaken to establish whether a full DPIA is required.

The following assessment will be used and staff will undergo training in order to effectively use the DPIA:

- DPIA Screening - Questions.docx
- ALL new assessments will be saved in the relevant programme folders
- No new projects or programmes will be signed off until the DPIA screening questions have been completed when deemed required. Based on the result of the screening, the DPO and project lead will decide if a further DPIA is required

Data Minimisation

We will be able to justify the need for Personal Data for each field/item, at each point of data collection, according to the purpose(s) we are seeking to achieve.

Accurate Personal Data

We adopt the following measures to maintain the accuracy of Personal Data:

- “Not at this address” returns are updated in the CRM within 4 weeks.
- “Hard bounces” of email addresses are updated in the CRM within 4 weeks.
- An annual “data accuracy” audit is run to improve the accuracy of data.

Re-using Personal Data

The process for assessing re-use requests is that staff will consult the DPO and the Director of their Team. Consistent criteria for access the request will be used based on the purpose and compatibility assessment tool.

Records Management

Record storage, retention and disposal

We have a Records and Retention Policy (in development for use by September 2021)

- This is based on legal requirements and industry standards, best practice or archival needs.
- In the absence of guidance from these sources, the legitimate business needs of the organisation for the particular purpose will be assessed by senior management and a decisions made on the appropriate retention period for the relevant records.
- The policy will define the locations and/or stores approved for records containing Personal Data, in both electronic and physical formats.

Note: Records will be disposed of securely.

Organisational Transparency

Privacy Policy

We will make accessible a Privacy Policy containing the privacy information required by Article 13 of the GDPR.

- As a minimum, this will be accessible via our website.
- This will be structured as follows:
    - A main Privacy Policy
    - Individual Policies for different audiences.

We will make accessible a Cookie Policy containing the information about our use of cookies as required by the Privacy and Electronic Communication Regulations. This will be done by the end September as we are currently undergoing a complete rebuild of the Foundation’s website.

- Consent will be obtained for non-essential cookies.

Privacy Notices

We will ensure that all points at which Personal Data is collected will have a Privacy Notice.

- Each Privacy Notice will contain sufficient privacy information to inform the Data Subject about the essential and/or unexpected collection and use of their Personal Data.
- The External Affairs Team and the Entrepreneurship Team are working together to provide privacy policies in the national language/s of the countries in which we work. This will be completed by September 2021.

A log of Privacy Notices will be maintained. This log

- Lists the current and historic Privacy Notices – including those in foreign languages
- Contains copies, or links to, each Privacy Notice
- Details who reviewed and authorised the Privacy Notice

Privacy Notices and consent collections will be reviewed by the DPO before they are used.

Where Personal Data is collected on the basis of Legitimate Interests, the decision-making process is as follows:

- Legitimate Interests Assessments (LIA) will be completed when required.
- The DPO will sign off LIAs.
- We will collect consent for photographs and video footage using this form.

Providing individuals with access to their Personal Data

A log of individual rights requests is maintained, and reported on as part of our performance and risk monitoring

- Please see log here.

Right of Subject Access

We ensure that Data Subjects are informed of their right to access their Personal Data and the options available to them for exercising this right by including this right in our privacy information.

- Requests are handled by the DPO, who will seek expert advice.

Right of data portability

We ensure that Data Subjects are informed of their right to data portability where it applies, and the options available to them for exercising this right by including this right in our privacy information.

- Requests are handled by the DPO, who will seek expert advice.

Enabling individuals to manage their Personal Data

Right to object

We ensure that Data Subjects are informed of their right to object as it applies to their Personal Data; by including this right in our privacy information.

The following procedure is followed for handling objections (this covers (i) direct marketing (ii) processing based on legitimate interests and (iii) processing based on public interest)

- Objections to direct marketing are handled by the Partnerships or External Affairs Departments
- Other objections are handled by the DPO, who will seek expert advice.

Right to erasure

We ensure that Data Subjects are informed of their right to erasure, where it applies, by including this right our privacy information.

- Requests are handled by the DPO, who will seek expert advice.

Right to rectification

We ensure that Data Subjects are informed of their right to rectification and the options available to them for managing their own data by including this right our privacy information.

- Requests are handled by the DPO, who will seek expert advice.

Right to restriction of processing

We ensure that Data Subjects are informed of their right to restriction of processing, where it applies to their Personal Data, by including this right in our privacy information.

- Requests are handled by the DPO, who will seek expert advice.

Rights over automated decision-making

We ensure that Data Subjects are informed of their rights in relation to automated individual decision-making (including profiling) as it applies to their Personal Data by including this right our privacy information.

When an automated decision is challenged, the DPO will seek expert advice.
Note: When implementing processing which involves automated decision-making or profiling of individual which may have legal effects or similar, we will ensure that there are

appropriate safeguards for the individuals' rights and freedoms by considering and building in those safeguards as described in Data Protection Impact Assessment (DPIA)