BACK ON TRACK
Helping Injured Veterans
Registered Charity Number 1169764

DATA PROTECTION POLICY

Reviewed by: Trustees

Approved: December 2020

Next review date: December 2022

Contents

1. Aims

1.1 Our charity aims to ensure that all personal data collected about volunteers, beneficiaries, trustees, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

2.1 This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

2.2 It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

2.3 It also reflects the ICO's code of practice for the use of personal information.

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Telephone number It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Genetics • Health – physical or mental • Sex life or sexual orientation

Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

4.1 Our charity processes personal data relating to beneficiaries, staff, trustees, volunteers and others, and therefore is a data controller.

4.2 The charity is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

5.1 This policy applies to all charity members as well as external organisations or individuals working on our behalf. Anyone who does not comply with this policy may face disciplinary action.

6. Governing board

6.1 The board of trustees has overall responsibility for ensuring that our charity complies with all relevant data protection obligations.

7. Data protection officer

7.1 The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

7.2 They will report directly to the trustees with their advice and recommendations on charity data protection issues.

7.3 The DPO is contactable via enquiries@backontrack.london

7.4 A designated trustee (namely Paula Hall) acts as the representative of the data controller on a day-to-day basis.

8. Charity Trustees

8.1 Trustees are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the charity of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - o With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - o If they have any concerns that this policy is not being followed
    - o If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - o If they need to rely on or capture consent, draft a privacy notice or deal with data protection rights invoked by an individual.
    - o If there has been a data breach
    - o Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - o If they need help with any contracts or sharing personal data with third parties

9. Data protection principles

9.1 The GDPR is based on data protection principles that our charity must comply with.

9.2 The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

9.3 This policy sets out how the charity aims to comply with these principles.

10. Collecting personal data lawfulness, fairness and transparency

10.1 We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the charity can fulfil a contract with the individual, or the individual has asked the charity to take specific steps before entering into a contract
- The data needs to be processed so that the charity can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that the charity, as a public authority, can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of the charity or a third party (provided the individual's rights and freedoms are not overridden)
- The individual has freely given clear consent

10.2 For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

10.3 Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

Limitation, minimisation and accuracy

10.4 We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

10.5 If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

10.6 When charity members no longer need the personal data they hold; they must ensure it is deleted or anonymised. This will be done in accordance with the charity Data Retention Policy.

11. Sharing personal data

11.1 We will not normally share personal data with anyone else, but may do so where:

- There is an issue with beneficiary that puts the safety of our charity members at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services– for example, IT companies. When doing this, we will:
    - o Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - o Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - o Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

11.2 We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

11.3 We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our beneficiaries or charity members.

Subject access requests and other rights of individuals

12. Subject access requests

12.1 Individuals have a right to make a 'subject access request' to gain access to personal information that the charity holds about them.

This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

12.2 Subject access requests should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

12.3 If the charity receives a subject access request they must immediately forward it to the DPO.

13. Responding to subject access requests

13.1 When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

13.2 If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

13.3 A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

13.4 When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO

14. Other data protection rights of the individual

14.1 In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

14.2 Individuals should submit any request to exercise these rights to the DPO.

15. Photographs and videos

15.1 As part of our charitable activities, we may take photographs and record images of individuals.

15.2 We will obtain written consent from beneficiaries for photographs and videos to be taken of them for communication, marketing and promotional materials.

15.3 Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

16. Data protection by design and default

16.1 We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge

- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law

- Completing privacy impact assessments where the charity's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)

- Integrating data protection into internal documents including this policy, any related policies and privacy notices

- Regularly training members of the charity on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance

- Regularly conducting reviews to test our privacy measures and make sure we are compliant

17. Data security and storage of records

17.1 We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

17.2 In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use

- Papers containing confidential personal data must not be left on office desks, on HQ tables, pinned to notice/display boards, or left anywhere else where there is general access

- Where personal information needs to be taken off HQ site, charity staff must sign it in and out

- Passwords are used to access charity computers, laptops and other electronic devices. Charity members are reminded to change their passwords at regular intervals

- Encryption software is used to protect portable devices such as laptops

- Charity members who store personal information on their personal devices are expected to follow the same security procedures as for charity -owned equipment.

- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and is adequately protected.

18. Disposal of records

18.1 Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

18.2 For example, we will shred or incinerate paper-based records, and delete electronic files.

19. Personal data breaches

19.1 The charity will make all reasonable endeavours to ensure that there are no personal data breaches.

19.2 In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

19.3 When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person
- The theft of a charity laptop containing non-encrypted personal data about beneficiaries

20. Training

20.1 All charity staff and trustees (also referred to as charity members) are provided with data protection training as part of their induction process.

20.2 Data protection will also form part of continuing professional development, where changes to legislation, guidance or the trust's processes make it necessary.

21. Monitoring arrangements

21.1 The DPO is responsible for monitoring and reviewing this policy.

22.2 This policy will be reviewed at least every 2 years and shared with the full governing board.

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - o Lost
    - o Stolen
    - o Destroyed
    - o Altered
    - o Disclosed or made available where it should not have been
    - o Made available to unauthorised people
- The DPO will alert the chair of Trustees
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant charity members where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - o Loss of control over their data
    - o Discrimination
    - o Identify theft or fraud
    - o Financial loss
    - o Damage to reputation
    - o Loss of confidentiality
    - o Any other significant economic or social disadvantage to the individual(s) concerned
- If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the charity's computer system.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

    - o A description of the nature of the personal data breach including, where possible:
    - o The categories and approximate number of individuals concerned
    - o The categories and approximate number of personal data records concerned
    - o The name and contact details of the DPO
    - o A description of the likely consequences of the personal data breach
    - o A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

    - o The name and contact details of the DPO
    - o A description of the likely consequences of the personal data breach
    - o A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

    - o Facts and cause
    - o Effects
    - o Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

- Records of all breaches will be stored on the charity computer system.

- The DPO and allocated trustee will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

- We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.

- Members of the charity who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

- The DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.

- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.

- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.