



Date Issued:	January 2018
Approved by Board on	April 2022
Next review due:	April 2023

# DATA PROTECTION POLICY

Global Feedback Ltd

DATA PROTECTION POLICY.....	1
1. Purpose of the policy.....	1
2. About this policy .....	1
3. Definitions of data protection terms.....	2
4. Data protection principles .....	3
5. Processing data fairly and lawfully.....	3
6. Processing data for the original purpose .....	4
7. Personal data should be adequate and accurate .....	4
8. Not retaining data longer than necessary .....	4
9. Rights of individuals under the GDPR.....	5
10. Data security .....	5
11. Transferring Data Outside the EEA.....	6
12. Processing sensitive personal data.....	6
13. Notification .....	6
14. Monitoring and review of the policy .....	6

## 1. Purpose of the policy

1.1 Global Feedback Ltd and Global Feedback Ltd EU is/are committed to complying with privacy and data protection laws including:

- (a) the EU General Data Protection Regulation (“**the GDPR**”) and any related legislation which applies in the UK such as the UK GDPR and the Data Protection Act 2018;
  - (b) the Privacy and Electronic Communications Regulations (2003) in the UK and any successor or related legislation, including without limitation, E-Privacy Regulation 2017/0003 and the relevant aspects of the Dutch Telecommunications Act and any successor or related legislation; and
  - (c) all other applicable laws and regulations relating to the processing of personal data and privacy, including statutory instruments and, where applicable, the codes of practice issued by the Information Commissioner’s Office (“**ICO**”) or any other relevant supervisory authority such as the Dutch Data Protection Authority.
- (together “**the Legislation**”)

1.2 This policy sets out what we do to protect individuals’ personal data.

1.3 Anyone who handles personal data in any way on behalf of Global Feedback Ltd must ensure that we comply with this policy. Section 3 of this policy describes what comes within the definition of “personal data”. Any breach of this policy will be taken seriously and may result in disciplinary action or more serious sanctions.

1.4 This policy may be amended from time to time to reflect any changes in legislation, regulatory guidance or internal policy decisions.

## 2. About this policy

2.1 The types of personal data that we may handle include details of:

employees, trustees, supporters, volunteers, donors. The CRM used for contact details within Feedback is Salesforce and personnel records of staff are held in CharlieHR. Donor and supporter details are held in Engaging Networks, RSM2000 and Stripe (our payment gateways).

2.2 The Head of Operations is the data protection officer at Global Feedback Ltd and is responsible for ensuring compliance with the GDPR and with this policy. Any questions or concerns about this policy should be referred in the first instance to the data privacy officer who can be contacted at [privacy@feedbackglobal.org](mailto:privacy@feedbackglobal.org) or on 020 3051 8633.

Please read this in conjunction with the table that lists all the retention periods and lawful bases (see section 5 below) that apply to the different types and formats of data that is requested and stored by Feedback.

The table is held here: [GDPR FEEDBACK Data audit and retention periods.xlsx](#)

### 3. Definitions of data protection terms

3.1 The following terms will be used in this policy and are defined below:

3.2 **Data Subjects** include all living individuals about whom we hold personal data, for instance an employee or a supporter. A data subject need not be a UK or Dutch national or resident. All data subjects have legal rights in relation to their personal data.

3.3 **Personal Data** means any information relating to a living person who can be identified directly or indirectly from that information (or from that information and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). It can also include an identifier such as an identification number, location data, an online identifier specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

3.4 **Data Controllers** are the people who, or organisations which, decide the purposes and the means for which, any personal data is processed. They have a responsibility to process personal data in compliance with the Legislation. Global Feedback Ltd is the data controller of all personal data that we manage in connection with our work and activities.

3.5 **Data Processors** include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include other organisations such as website hosts, fulfilment houses or other service providers which handle personal data on our behalf.

3.6 **European Economic Area** includes all countries in the European Union as well as Norway, Iceland and Liechtenstein.

3.7 **ICO** means the Information Commissioner's Office (the authority which oversees data protection regulation in the UK).

3.8 **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.

**3.9 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

#### **4. Data protection principles**

4.1 Anyone processing personal data must comply with the six data protection principles set out in the EU GDPR/ UK GDPR. We are required to comply with these principles (summarised below), and show that we comply, in respect of any personal data that we deal with as a controller.

4.2 Personal data should be:

- (a) processed fairly, lawfully and transparently;
- (b) collected for specified, explicit and legitimate purposes and not further processed in a way which is incompatible with those purposes;
- (c) adequate, relevant and limited to what is necessary for the purpose for which it is held;
- (d) accurate and, where necessary, kept up to date;
- (e) not kept longer than necessary; and
- (f) processed in a manner that ensures appropriate security of the personal data.

#### **5. Processing data fairly and lawfully**

5.1 The first data protection principle requires that personal data is obtained fairly and lawfully and processed for purposes that the data subject has been told about. Processing will only be lawful if certain conditions can be satisfied, including where the data subject has given consent, or where the processing is necessary for one or more specified reasons, such as where it is necessary for the performance of a contract.

5.2 To comply with this principle, every time we receive personal data about a person directly from that individual, which we intend to keep, we need to provide that person with **“the fair processing information”**. In other words we need to tell them:

- (a) the type of information we will be collecting (categories of personal data concerned);
- (b) who will be holding their information, i.e. Global Feedback Ltd including contact details and the contact details of our Data Privacy Officer (if we have one);
- (c) why we are collecting their information and what we intend to do with it for instance to process donations or send them mailing updates about our activities;
- (d) the legal basis for collecting their information:
  - **Consent:** the individual has given clear consent to process their personal data for a specific purpose.
  - **Contract:** the processing is necessary for a contract with the individual,
  - **Legal obligation:** the processing is necessary to comply with the law.
  - **Vital interests:** the processing is necessary to protect someone's life.
  - **Public task:** the processing is necessary to perform a task in the public interest or official functions, with a clear basis in law.

- **Legitimate interests:** the processing is necessary for legitimate interests unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

(e) if we are relying on legitimate interests as a basis for processing what those legitimate interests are;

(f) whether the provision of their personal data is part of a statutory or contractual obligation and details of the consequences of the data subject not providing that data;

(g) the period for which their personal data will be stored or, where that is not possible, the criteria that will be used to decide that period;

(h) details of people or organisations with whom we will be sharing their personal data;

(i) if relevant, the fact that we will be transferring their personal data outside the UK or EEA and details of relevant safeguards; and

(j) the existence of any automated decision-making including profiling in relation to that personal data.

5.3 Where we obtain personal data about a person from a source other than the person his or herself, we must provide that individual with the following information **in addition to that listed under 5.2 above:**

(a) the categories of personal data that we hold; and

(b) the source of the personal data and whether this is a public source.

5.4 In addition, in both scenarios, (where personal data is obtained both directly and indirectly) we must also inform individuals of their rights outlined in section 9 below, including the right to lodge a complaint with the ICO or the Dutch Data Protection Authority and, the right to withdraw consent to the processing of their personal data.

5.5 This fair processing information can be provided in a number of places including on web pages, in mailings or on application forms. We must ensure that the fair processing information is concise, transparent, intelligible and easily accessible.

## **6. Processing data for the original purpose**

6.1 The second data protection principle requires that personal data is only processed for the specific, explicit and legitimate purposes that the individual was told about when we first obtained their information.

6.2 This means that we should not collect personal data for one purpose and then use it for another. If it becomes necessary to process a person's information for a new purpose, the individual should be informed of the new purpose beforehand. For example, if we collect personal data such as a contact number or email address, in order to update a person about our activities it should not then be used for any new purpose, for example to share it with other organisations for marketing purposes, without first getting the individual's consent.

## **7. Personal data should be adequate and accurate**

The third and fourth data protection principles require that personal data that we keep should be accurate, adequate and relevant. Data should be limited to what is necessary in relation to the purposes for which it is processed. Inaccurate or out-of-date data should be destroyed securely, and we must take every reasonable step to ensure that personal data which is inaccurate is corrected.

## **8. Not retaining data longer than necessary**

8.1 The fifth data protection principle requires that we should not keep personal data for longer than we need to for the purpose it was collected for. This means that the personal data that we hold should be destroyed or erased from our systems when it is no longer needed. If you think that we are holding out-of-date or inaccurate personal data, please speak to the Data Privacy Officer.

8.2 For guidance on how long particular types of personal data that we collect should be kept before being destroyed or erased, please contact the Data Privacy Officer or seek legal advice.

## **9. Rights of individuals under the EU GDPR and UK GDPR**

9.1 The EU GDPR/ UK GDPR gives people rights in relation to how organisations process their personal data. Everyone who holds personal data on behalf of Global Feedback Ltd needs to be aware of these rights. They include (but are not limited to) the right:

- (a) to request a copy of any personal data that we hold about them (as controller), as well as a description of the type of information that we are processing, the uses that are being made of the information, details of anyone to whom their personal data has been disclosed, and how long the data will be stored (known as subject access rights);
- (b) to be told, where any information is not collected from the person directly, any available information as to the source of the information;
- (c) to be told of the existence of automated decision-making;
- (d) to object to the processing of data where the processing is based on either the conditions of public interest or legitimate interests;
- (e) to have all personal data erased (the right to be forgotten) unless certain limited conditions apply;
- (f) to restrict processing where the individual has objected to the processing;
- (g) to have inaccurate data amended or destroyed; and
- (h) to prevent processing that is likely to cause unwarranted substantial damage or distress to themselves or anyone else,

If you receive an individual rights request from a data subject regarding any of the above please forward it to [privacy@feedbackglobal.org](mailto:privacy@feedbackglobal.org)

## **10. Data security**

10.1 The sixth data protection principle requires that we keep secure any personal data that we hold.

10.2 We are required to put in place procedures to keep the personal data that we hold secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

10.3 When we are dealing with sensitive personal data, more rigorous security measures are likely to be needed, for instance, if sensitive personal data (such as details of an individual's health, race or sexuality) is held on a memory stick or other portable device it should always be encrypted.

10.4 When deciding what level of security is needed, your starting point should be to look at whether the information is sensitive or highly confidential and how much damage could be caused if it fell into the wrong hands.

10.5 The following security procedures and monitoring processes must be followed in relation to all personal data processed by us: measures to restore availability and access to data in a timely manner in event of physical or technical incident; process for regularly testing, assessing and evaluating effectiveness of security measures; backing up data (daily back-ups should be taken of all data on the system and data should not be stored on local drives or removable media as these will not be backed up); entry controls (any stranger seen in entry-controlled areas should be reported); staff should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended; paper documents should be shredded, memory sticks, CD-ROMs and other media on which personal data is stored should be physically destroyed when they are no longer required (remote workers will need to provide evidence that the data has been destroyed such a video or photographic evidence of its destruction); desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential) and staff must keep data secure when travelling or using it outside the offices.

## **11. Transferring Data Outside the EEA or UK**

11.1 The UK GDPR requires that when organisations transfer personal data outside the EEA or UK, they take steps to ensure that the data is properly protected.

11.2 The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and the LED, and Uruguay as providing adequate protection. Please refer to this list for the latest updates: [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en)

11.3 As such, personal data may be transferred to people or organisations in these countries without the need to take additional steps beyond those you would take when sharing personal data with any other organisation. In transferring personal data to other countries outside the UK or EEA (which are not on this approved list), it will be necessary to enter into an ICO or UK Government-approved agreement, seek the explicit consent of the individual, or rely on one of the other derogations under the UK GDPR that apply to the transfer of personal data outside the UK or the EEA. Please refer to [these](#) documents from the ICO for information regarding international data transfer agreement and guidance.

11.4 For more information, please speak to the data protection officer or seek further legal advice.

## **12. Processing sensitive personal data**

12.1 On some occasions we may collect information about individuals that is defined by the GDPR as **special categories of personal data**, and special rules will apply to the processing of this data. In this policy we refer to “special categories of personal data” as “sensitive personal data”. The categories of sensitive personal data are set out in the definition in Section 3.9. This sensitive personal data would be collected through supporter surveys which would be anonymous and not personally identifiable.

12.2 Purely financial information is not technically defined as sensitive personal data by the EU GDPR/ UK GDPR. However, particular care should be taken when processing such data, as the ICO and Dutch Data Protection Authority will also treat a breach relating to financial data very seriously.

12.3 In most cases, in order to process sensitive personal data, we must obtain explicit consent from the individuals involved. As with any other type of information we will also have to be absolutely clear with people about how we are going to use their information.

12.4 It is not always necessary to obtain explicit consent. There are a limited number of other circumstances in which the EU GDPR/ UK GDPR permits organisations to process sensitive personal data. If you are concerned that you are processing sensitive personal data and are not able to obtain explicit consent for the processing, please speak to the data protection officer.

## **13. Notification**

13.1 We recognise that whilst there is no obligation for us to make an annual notification to the ICO under the UK GDPR, we will consult with the ICO where necessary when we are carrying out “high risk” processing.

13.2 We will report breaches (other than those which are unlikely to be a risk to individuals) to the ICO where necessary, within 72 hours. We will also notify affected individuals where the breach is likely to result in a high risk to the rights and freedoms of these individuals. If you are the cause of or involved in a data security breach you must call the Head of Operations immediately to notify them of the breach, they will either contact the ICO or instruct you on what to do next.

## **14. Training staff about this policy**

It is essential that all staff and volunteers are made aware of the need and reason for maintaining confidentiality. All staff and volunteers will be required to read and understand the Data Protection Policy as part of their induction.

### **15. Enforcement of the policy/breaches of confidentiality**

Feedback regards any breach of this policy as a serious issue and will take action as set out in this section.

Feedback acknowledges that most breaches of confidentiality occur not out of malice but through thoughtlessness, or lack of awareness of the consequences of an action. Feedback recognises that further training may be the most appropriate response in some circumstances.

All Feedback staff and volunteers and interns are expected to sign a contract or volunteer agreement which expects them to work within the organisation's policies and procedures.

### **16. Monitoring and review of the policy**

14.1 This policy along side the GDPR FEEDBACK Data audit and retention periods.xlsx table is reviewed annually by our board of trustees to ensure that it is achieving its objectives.