Data Protection Policy

Approved by the Globethics Board of Foundation on 29 April 2022

Contents

1. Legal notice **2**

2. Why this policy exists **2**

3. Data protection rules **2**

4. People, risks and responsibilities **3**

Policy scope 3

Data protection risks 4

Responsibilities 4

5. General staff guidelines **5**

6. Data storage **5**

7. Data use **6**

8. Data accuracy **6**

9. Subject access requests **7**

10. Disclosing data for other reasons **7**

11. Providing information **7**

1. Legal notice

This data protection policy draws upon and complements the Globethics Privacy Policy and the Globethics Terms of Service Agreement.

Globethics operates in accordance with the Globethics Code of Ethics and is guided by the vision, mission and core values of the organisation, which are reflected in this data protection policy.

Globethics with its Head Office in Geneva, Switzerland, constituted in accordance with Art. 80 et seq. of the Swiss Civil Code and subject to Swiss federal law operates in accordance with Swiss Federal Act on Data Protection (1992) and the Canton of Geneva legislation on data protection and transparency (2002).

The data protection policy is governed by the European Union's General Data Protection Regulation (GDPR, 2018) that enshrines data protection to private citizens within the EEA.

Globethics shall not be held liable for the practices of any third parties, either directly or inferred.

2. Why this policy exists

Globethics needs to gather and use information about individuals. These can include those individuals the organisation serves, suppliers, contacts, employees and other people the organisationhas a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the organisation's data protection standards and to comply with the law.

This data protection policy ensures that Globethics:

- Complies with data protection legislation and follows good practice;
- Protects the rights of staff, mandate holders, beneficiaries and partners;
- Is open about how it stores and processes individuals' data; and
- Protects itself from the risks of a data breach

3. Data protection rules

Data protection laws and legislation describe how organisations — including Globethics— must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The following principles serve to guide in the processing, storage and use of personal data.

Data must:

1. Be processed fairly and lawfully;
2. Be obtained only for specific, lawful purposes;
3. Be adequate, relevant and not excessive;
4. Be accurate and kept up to date;
5. Not be held for any longer than necessary;
6. Processed in accordance with the rights of data subjects;
7. Be protected in appropriate ways; and
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

4. People, risks and responsibilities

Policy scope

This policy applies to:

- The Globethics Head Office;
- All Globethics branches and regional and national offices;
- All staff, volunteers, interns, mandate holders, associates, advisors and Board and committeemembers of Globethics; and
- All contractors, suppliers and other people working on behalf of Globethics.

It applies to all data that the organisation holds relating to identifiable individuals. This can include:

- Names of individuals;
- Postal addresses;
- Email addresses;
- Telephone numbers; and
- Any other information relating to individuals

Data protection risks

This policy helps to protect Globethics from data security risks, including:

- Breaches of confidentiality, for instance, information being given out inappropriately;
- Failing to offer choice, for instance, all individuals should be free to choose how theorganisation uses data relating to them; and
- Reputational damage, for instance, the organisation could suffer if hackers successfully gainedaccess to sensitive data.

Responsibilities

Everyone who works for or with Globethics has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person and/or team that handles personal data must ensure that it is handled and processed inline with this policy and data protection principles.

However, the following people have key areas of responsibility:

- The Board of Foundation is ultimately responsible for ensuring that Globethics meets itslegal obligations.
- The Head of Support and Development Department is responsible for:
  - Keeping the board updated about data protection responsibilities, risks and issues;
  - Reviewing all data protection procedures and related policies, in line with an agreedschedule in the framework of the Internal Control System;
  - Arranging data protection training and advice for the people covered by this policy;
  - Handling data protection questions from staff and anyone else covered by this policy;
  - Dealing with requests from individuals to see the data Globethics holds about them (also called 'subject access requests'); and
  - Checking and approving any contracts or agreements with third parties that may handle the organisation's sensitive data.
- The Administration and Human Resources Manager together with the Head of Support and Development Department and service providers contracted for this purpose are responsible for:
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards;
  - Performing regular checks and scans to ensure security hardware and software isfunctioning properly; and
  - Evaluating any third-party services the organisation is considering using to store or processdata, for instance, cloud computing services.

- The Communications and Digital Marketing Manager is responsible for:
  - Ensuring that any data protection statements attached to communications such as emails and letters are approved;
  - Answering any data protection queries from journalists or media outlets like newspapers; and
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

5. General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Globethics will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the Head of Support and Development Department if they are unsure about any aspect of data protection.

6. Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Administration and Human Resources Manager or the Head of Support and Development Department.

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

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

- When not required, the paper or files should be kept in a locked drawer or filing cabinet;
- Employees should make sure paper and printouts are not left where unauthorised people could see them, for instance on a printer; and
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees;
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used;
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services;
- Servers containing personal data should be sited in a secure location, away from general office space;
- Data should be backed up frequently. Those backups should be tested regularly, in line with the organisation's standard backup procedures;
- Data should never be saved directly to laptops or other mobile devices like tablets or smartphones; and
- All servers and computers containing data should be protected by approved security software and a firewall.

7. Data use

Personal data is of no value to Globethics unless the organisation can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended;
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure;
- Data must be encrypted before being transferred electronically to authorised external contacts;
- Personal data should never be transferred outside of the European Economic Area; and
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

8. Data accuracy

Globethics is required to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort that Globethics should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated, for instance, by confirming a contact's details when they call.
- Globethics will make it easy for data subjects to update the information Globethics holds about them, for instance, via the organisation's website.
- Data should be updated as inaccuracies are discovered, for instance, if a contact can no longer be reached on their stored telephone number, it should be removed from the database.

9. Subject access requests

All individuals who are the subject of personal data held by Globethics are entitled to:

- Ask what information the organisation holds about them and why;
- Ask how to gain access to it;
- Be informed how to keep it up to date; and
- Be informed how the organisation is meeting its data protection obligations.

If an individual contacts the organisation requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to infoweb@globethics.net.

The organisation will aim to provide the relevant data within 14 days after verifying the identity of anyone making a subject access request before handing over any information.

10. Disclosing data for other reasons

In certain circumstances, the laws and legislation in force allow personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Globethics will disclose the data requested. However, the organisation will ensure the request is legitimate, seeking assistance from the Board of Foundation and requesting legal advice where necessary.

11. Providing information

Globethics aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used; and
- How to exercise their rights.

To these ends, the organisation has a Privacy Policy and a Terms of Service Agreement, setting out how data relating to individuals is used by the organisation. Both of these documents are available on the organisation's website.