DATA PROTECTION POLICY

Implementing the EU General Data Protection Regulation

Table of Contents

1. INTRODUCTION

FRIENDS OF THE EARTH need to collect and use certain types of information about its Members, Associates and other Individuals or Business Associates (hereinafter referred to as “Users”) who come into contact with FRIENDS OF THE EARTH in order to carry on their activity. This personal information must be collected and dealt with appropriately whether it is collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this under Regulation EU 2016/679 (hereinafter referred to as the GDPR).

As a global trend, Data Privacy Laws are becoming stricter, including the penalties for non-compliance. The purpose of this policy is to facilitate FRIENDS OF THE EARTH’ compliance with Data Privacy Laws worldwide by ensuring that adequate procedures and practices are in place relating to the processing of personal data.

This Data Protection Policy sets out how FRIENDS OF THE EARTH (”we”, “our”, “us”, “FRIENDS OF THE EARTH”) handle the Personal Data of our members, suppliers, employees and other third parties.

This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present members, employees or supplier contacts, website users or any other Data Subject.

This Data Protection Policy also applies to all Personnel (”you”, “your”). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements. This Data Protection Policy sets out what we expect from you in order for the Organisation to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Data Protection Policy. You must also comply with all such Related Policies and Privacy Guidelines. **Any breach of this policy will be taken seriously and any breach of this Data Protection Policy may result in disciplinary action.**

This Data Protection Policy (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties without prior authorisation from the Management.

This Code of Practice has been approved by FRIENDS OF THE EARTH as part of their commitment to their legal duties and the highest standards of information governance.

2. DATA CONTROLLER

FRIENDS OF THE EARTH are the Data Controller under the Regulation, which means that they determine what purposes personal information held, will be used for. They are also responsible for notifying the Information Commissioner of the data they hold or are likely to hold, and the general purposes that this data will be used for.

3. SCOPE – POLICY STATEMENT

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Organisation is exposed to potential fines of up to 20 000 000 EUR or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

All members of management are responsible for ensuring all Organisation Personnel comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance. This policy applies to all FRIENDS OF THE EARTH personnel.

Please contact the Data Protection Officer with any questions about the operation of this Data Protection Policy or the GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always contact the Data Protection Officer in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Organisation);

(b) if you need to rely on Consent and/or need to capture Explicit Consent;

(c) if you need to draft Privacy Notices or Fair Processing Notices;

(d) if you are unsure about the retention period for the Personal Data being Processed;

(e) if you are unsure about what security or other measures you need to implement to protect Personal Data;

(f) if there has been a Personal Data Breach;

(g) if you are unsure on what basis to transfer Personal Data outside the EEA;

(h) if you need any assistance dealing with any rights invoked by a Data Subject;

(i) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA or plan to use Personal Data for purposes others than what it was collected for;

(j) If you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making;

(k) If you need help complying with applicable law when carrying out any activities; or

(l) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors).

4. PERSONAL DATA PROTECTION PRINCIPLES

Data Privacy Laws typically apply to “personal data” (also known as “personal information” or “personally identifiable information”).

Personal data means any information relating to an identified or identifiable living individual.

Examples of personal data include names, dates of birth, addresses, social security and identity card numbers. It also includes IP addresses, location data, health, economic, cultural or social information, as well as expressions of opinion about an individual (such as HR appraisal records).

Personal data may relate to employees, members of the Board, job applicants or individual contacts at third parties and business contacts. If information can be linked to an individual in some way, it will likely be personal data. A broader range of information than you may expect can be personal data. Here are some more specific examples:

An employee: All information submitted by the employee, such as their phone number and addresses, will be the employee's personal data. FRIENDS OF THE EARTH record of any discussions about the employee's qualifications, personality or performance at work (whether in email or in specific records) will also be the employee's personal data.

A business contact: If FRIENDS OF THE EARTH Personnel got in touch with a business contact (e.g. at a meeting or a trade fair), and then subsequently sent an internal email for business development purposes which mentioned contact details or any non-business information about the business contact (e.g. opinions about the contact, or information about their family, interests outside work, favourite food etc.) that information would be the business contact's personal data.

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).
(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).
(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).
(d) Accurate and where necessary kept up to date (Accuracy).
(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).
(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).
(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).
(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

What personal data do FRIENDS OF THE EARTH collect and for what purposes?

FRIENDS OF THE EARTH collects personal data relating to:

(a) Employees and directors, including relevant persons' contact details, passport details, job application, records of training, documentation of performance appraisals, salary details, expense claims, education, other employment records, and, with respect to directors only, health conditions (Employee Personal Data);

(b) Business contact names, contact details and sometimes passport details (Business Contact Personal Data); this includes client data;

(c) Members' personal data (including names, passport/ID information, financial information etc.) for the purpose of the provision of services to our members and for regulatory / legal and/or compliance purposes according to the applicable laws where we operate.

FRIENDS OF THE EARTH hold and process these categories of personal data for the following main purposes:

(a) Employee Personal Data for the administration and management of FRIENDS OF THE EARTH personnel, including recruiting, benefits and entitlements;

(b) Client personal data (including names, passport/ID information, financial information etc.) for the purpose of the provision of services to our members and for regulatory / legal and/or compliance purposes according to the applicable laws where we operate.

(c) Business Contact Personal Data for the administration and management of our relationships with our cooperation partners and suppliers; and

(d) All categories of personal data to comply with applicable laws, regulations and rules, including without limitation providing such data to the regulatory authorities Authority and other state regulators on request and disclosing client fund and/or financial details if applicable.

5. LAWFULNESS, FAIRNESS, TRANSPARENCY

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the

Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her Consent;
(b) the Processing is necessary for the performance of a contract with the Data Subject;
(c) to meet our legal compliance obligations;
(d) to protect the Data Subject's vital interests; or
(e) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notice.

You must identify and document the legal ground being relied on for each Processing activity

6. DISCLOSURE

FRIENDS OF THE EARTH may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Users will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows FRIENDS OF THE EARTH to disclose data (including sensitive data) without the data subject's consent.

These are:

a) Carrying out a legal duty under Cyprus or EU Law, as instructed by any Court of Law or as authorised by the relevant authorities to disclose information about a certain individual, individuals and/or corporate information;

b) Protecting vital interests of Users or other person;

c) The User has already made the information public;

d) Conducting any legal proceedings, obtaining legal advice or defending any legal rights;

e) Monitoring for equal opportunities purposes – i.e. race, disability or religion;

f) Providing a confidential service where User's consent cannot be obtained or where it is reasonable to proceed without consent.

FRIENDS OF THE EARTH regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom they deal.

FRIENDS OF THE EARTH intend to ensure that personal information is treated lawfully and correctly.

To this end, FRIENDS OF THE EARTH will adhere to the Principles of Regulation EU 2016/679 - The EU General Data Protection Regulation.

Specifically, the Principles require that personal information:

a) Shall be obtained and processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;

b) Shall be obtained only for one or more of the purposes specified in the Regulation, and shall not be processed in any manner incompatible with that purpose or those purposes;

c) Shall be adequate, relevant and not excessive in relation to those purpose(s);

d) Shall be accurate and, where necessary, kept up to date;

e) Shall not be kept for longer than is necessary for the purpose;

f) Shall be processed in accordance with the rights of data subjects under the Regulation;

g) Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information;

h) Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Users in relation to the processing of personal information.

FRIENDS OF THE EARTH will, through appropriate management and strict application of criteria and controls**:**

- Observe fully conditions regarding the fair collection and use of information;

- Meet its legal obligations to specify the purposes for which information is used;
- Collect and process appropriate information, and only to the extent that it is needed to fulfill its operational needs or to comply with any legal requirements;
- Ensure the quality of information used
- Ensure that the rights of people about whom information is held, can be fully exercised under the Regulation. These include:
    - The right to be informed that processing is being undertaken,
    - The right of access to one's personal information'
    - The right to prevent processing in certain circumstances and
    - The right to correct, rectify, block or erase information which is regarded as wrong information)
- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred abroad without suitable safeguards.
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.
- Set out clear procedures for responding to requests for information.

7. DATA COLLECTION

Informed consent is when:

- A User clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data.
- And then gives their consent.

FRIENDS OF THE EARTH will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, FRIENDS OF THE EARTH will ensure that the User:

a) Clearly understands why the information is needed;

b) Understands what it will be used for and what the consequences are should the User decide not to give consent to processing;

c) As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed;

d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress;

Has received sufficient information on why their data is needed and how it will be used.

8. DATA STORAGE

Information and records relating to service users will be stored securely and will only be accessible to authorised staff and volunteers.

- Members' Data will only be stored digitally in specially designated folders in which only authorised staff shall have access.
- When appointing an external Data Processor, FRIENDS OF THE EARTH, shall only use Data Processors that will guarantee to implement appropriate technical and organisational measures in order to ensure that their processing activities met the requirements of the law and this Policy and ensure the protection of the rights of Data Subjects.
- Employee personal and sensitive data will only be handled by the Board of Directors.

Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately.

It is the responsibility of FRIENDS OF THE EARTH to ensure all personal and Organisation data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

9. STORAGE LIMITATION – RETENTION PERIODS

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The Organisation will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

DATA RETENTION PERIODS	
EMPLOYEE DATA	7 YEARS from termination of employment
CANDIDATE DATA	1 YEAR from receipt of CV/Application Form
MEMBERS DATA	2 YEARS from last contact
BUSINESS CONTACTS	7 YEARS from last contact

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Organisation's applicable records retention schedules and policies as those are listed above. This includes requiring third parties to delete such data where applicable.

You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice or Fair Processing Notice.

10. REPORTING A PERSONAL DATA BREACH

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable

Regulator and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Data Protection Officer and follow the SECURITY INCIDENT RESPONSE PLAN, which can be found in the Data Protection Office folder. You should preserve all evidence relating to the potential Personal Data Breach

What is a Data Breach?

A “data breach” typically includes a situation where personal data is, accidentally or unlawfully, lost, destroyed, altered, disclosed or accessed (or is exposed to any other form of unlawful processing).

Examples of a data breach are:

(a) loss or theft of an unencrypted USB stick, laptop or mobile phone;
(b) an intrusion or theft by a hacker;
(c) sending of a mass email where the email addresses of all recipients are mistakenly visible to all other recipients; and
(d) loss of personal data due to a crashing IT system.

It is very important that a data breach is reported internally immediately. In many cases, FRIENDS OF THE EARTH will have to report the data breach to a data privacy regulator within a specified timeframe. For example, in the European Union FRIENDS OF THE EARTH must, generally, notify the relevant regulator of a data breach no later than 72 hours after it becomes aware of that breach – if FRIENDS OF THE EARTH do not comply with this requirement, it must be able to provide reasons for not doing so. Late reporting or failure to report may result in serious adverse consequences for FRIENDS OF THE EARTH. In some circumstances, FRIENDS OF THE EARTH will also be required to notify affected Data Subjects of a data breach, in particular where such breach is likely to result in a high risk to the rights and freedoms of the relevant Data Subject or other individuals.

Furthermore, FRIENDS OF THE EARTH must maintain a record of the data breaches that have occurred in respect of any personal data held by FRIENDS OF THE EARTH or by a Data Processor on behalf of FRIENDS OF THE EARTH. This record must include details of all data breaches that are subject to breach notification requirements (as assessed by the Managing Director of FRIENDS OF THE EARTH), including in respect of each data breach:

(a) a description of the facts and circumstances of the breach; and

(b) whether or not the Data Subject(s) has/have been notified of the breach.

It is good practice to record the same information for data breaches that FRIENDS OF THE EARTH have decided are not subject to the breach notification requirements (as well as the justification for reaching this conclusion).

In practice, the obligation to maintain an overview of data breaches will likely be satisfied by retaining copies of all breach notifications submitted to the relevant data privacy regulator.

11. TRANSFER LIMITATION

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

You may only transfer Personal Data outside the EEA if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms as those are listed on the EU Website: https://ec.europa.eu/info/law/law-topic/data-protection_en ;
(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;
(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
(d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

12. DATA SUBJECT'S RIGHTS AND REQUESTS

Data Subjects have rights when it comes to how we handle their Personal Data. These

include rights to:

(a) withdraw Consent to Processing at any time;
(b) receive certain information about the Data Controller's Processing activities;
(c) request access to their Personal Data that we hold;
(d) prevent our use of their Personal Data for direct marketing purposes;
(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
(f) restrict Processing in specific circumstances;
(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;
(i) object to decisions based solely on Automated Processing, including profiling (ADM);
(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
(l) make a complaint to the supervisory authority; and
(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to the DPO and comply with the Organisation's Data Subject response process.

13. RECORD KEEPING

The GDPR requires us to keep full and accurate records of all our data Processing activities.

You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents in accordance with the Organisation's record keeping guidelines.

These records should include, at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

14. TRAINING AND AUDIT

We are required to ensure all Organisation Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.

You must regularly review all the systems and processes under your control to ensure they comply with this Privacy Standard and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

15. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with data privacy principles.
You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

a) the state of the art;

b) the cost of implementation;
c) the nature, scope, context and purposes of Processing; and
d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing. Data controllers must also conduct DPIAs in respect to high risk Processing. You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:
e) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
f) Automated Processing including profiling and ADM;
g) large scale Processing of Sensitive Data; and
h) large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

a. a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;
b. an assessment of the necessity and proportionality of the Processing in relation to its purpose;
c. an assessment of the risk to individuals; and
d. the risk mitigation measures in place and demonstration of compliance.

16. SHARING PERSONAL DATA

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of our group if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

17. CHANGES TO THIS DATA PROTECTION POLICY

We reserve the right to change this Data Protection Policy at any time without notice to you so please check back regularly to obtain the latest copy of this Privacy Standard. We issued this Privacy Standard on 10 May 2018 and no changes have been made since then.

This Privacy Standard does not override any applicable national data privacy laws and regulations in countries where we operate.

18. DATA ACCESS AND ACCURACY

All Users have the right to access any personal data that is being held about them by FRIENDS OF THE EARTH. This right can be exercised by applying in writing to the Data Protection Officer.

FRIENDS OF THE EARTH will also take reasonable steps to ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition**,** FRIENDS OF THE EARTH will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection.
- Everyone processing personal information understands that they are contractually responsible for following good data protection practice.
- Everyone processing personal information is appropriately trained to do so.
- Everyone processing personal information is appropriately supervised.

- Anybody wanting to make enquiries about handling personal information knows what to do.
- It deals promptly and courteously with any enquiries about handling personal information.
- It describes clearly how it handles personal information.
- It will regularly review and audit the ways it hold, manage and use personal information.
- It regularly assesses and evaluates its methods and performance in relation to handling personal information.
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them and may be considered gross misconduct in some cases.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the GDPR.

In case of any queries or questions in relation to this policy, please contact the FRIENDS OF THE EARTH Data Protection Officer:

Name of DPO IF applicable

Signed: Position: Date: Review Date:

Glossary of Terms

Data Controller – The person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Organisation Personnel and Personal Data used in our business for our own commercial purposes

Data Subject - a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Regulation EU 2016/679 - The EU General Data Protection Regulation– The EU legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person(s) responsible for ensuring that FRIENDS OF THE EARTH follow their data protection policy and comply with Regulation EU 2016/679.

Personal Data Breach - any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design - implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Code of Conduct - the Organisation privacy/GDPR related guidelines provided to assist in interpreting and implementing this policy.

User – The person whose personal information is being held or processed by FRIENDS OF THE EARTH for example: a member, an employee, or business associate.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them. **Explicit consent** is required for processing sensitive data.

Notification – Notifying the Data Protection Commissioner about the data processing activities of FRIENDS OF THE EARTH, as certain activities may be exempt from notification.

Office of the Commissioner for Personal Data Protection – The Cyprus Personal Data Protection Commissioner responsible for implementing and overseeing the Regulation EU 2016/679.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees within (GROUP).

Sensitive Personal Data - information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions. Criminal record or proceedings

DATA PROTECTION GUIDELINES

- **Tell people what you are doing with their data**
  People should know what you are doing with their information and who it will be shared with. This is a legal requirement (as well as established best practice) so it is important you are open and honest with people about how their data will be used.

- **Consider how people would feel about us holding their data**
  One way to help you follow the data protection principles (se e section **Error! Reference source not found.**) is to ensure that the individual concerned would not be surprised or upset by any information you hold about them or anything you do with their information.

- **Use strong passwords, and keep them secret**
  There is no point protecting the personal data you hold with a password if that password is easy to guess. Keep passwords secret – never disclose them over email, not even to IT.

- **Think about physical security**
  Know who is in the building (i.e. visitors, volunteers, cleaners, third party contractors etc.). Any unauthorised person seen in entry-controlled areas should be immediately reported to your line manager.

- **Secure lockable desks and cupboards**
  Ensure that physical records and IT equipment are secure by locking your computer when away from your desk and keeping filing cabinets locked.

- **Encrypt all portable devices, such as memory sticks and laptops**

- **Be mindful of what you are recording**
  FRIENDS OF THE EARTH Personnel, members and any other individuals whose personal data FRIENDS OF THE EARTH hold have rights to see their personal data. As a general rule, you should not put anything in writing that you would not want to be disclosed to the Data Subject.

- **Only keep people's data for as long as necessary**

- **Be careful when dealing with enquiries from third parties**
  If you receive an ad-hoc enquiry from a third party, be careful about disclosing any personal data held by FRIENDS OF THE EARTH. Check the identity of the person

making the enquiry and that they are legally entitled to the information they have requested. Consider whether a written data sharing contract is needed.

- **Report data breaches**
  Any loss or compromise of data should be reported to **the Managing Director of FRIENDS OF THE EARTH** immediately. This could be in a number of forms, such as a hack or a loss of a laptop or other device.

- **Make sure your staff are adequately trained**
  New employees must receive data protection training to explain how they should store and handle personal data. Refresher training should be provided at regular intervals for existing staff.

- **Speak to Legal and/or Compliance Department if you have any queries**

Acknowledgement of receipt of Data Protection Compliance Policy

---

Acknowledgement slip

Please complete this form and return to the DPO

I hereby acknowledge receipt of Data Protection Compliance Policy of FRIENDS OF THE EARTH (the Organisation) dated the XXXXXX XXXXXXXXX XXXX (the Policy). I confirm that I read the Policy and its content is clear to me. I acknowledge that the Policy may be amended by the Organisation from time to time in accordance with the regulatory requirements, and I understand that my personal data will be processed in accordance with such requirements as amended.

I hereby consent to the collection and processing of my personal data by FRIENDS OF THE EARTH in accordance with its Data Protection Policy.

_____

Signature

Name: …….

Position: ……

Department: …….

Date: …….