EIA UK Data Protection Policy

Data Controller: Environmental Investigation Agency UK, Company No. 7844550

This policy applies to:

- the UK office of the Environmental Investigation Agency UK (EIA UK)
- the UK office of the Environmental Investigation Agency Charitable Trust, UK Registered Charity No. 1145359
- to paid staff and volunteers of EIA UK
- to any other personnel operating on behalf of EIA UK.

Both legal entities are registered with the Information Commissioner for the United Kingdom and are referred to as EIA UK in this policy. Processing and retention of personal information is governed by the Data Protection Act 2018 and the EU General Data Protection Regulation (GDPR), which came into effect on 25 May 2018 GDPR.

[This policy does not apply to Environmental Investigation Agency Inc, which is a not-for-profit organisation based in the USA and therefore not within the jurisdiction of UK legislation.]

1. Purpose of the policy

The purpose of this policy is to enable EIA UK to:

- comply with the law in respect of the data it holds about individuals
- follow good practice
- protect EIA UK's supporters, staff and other individuals
- protect the organisation from the consequences of a breach of its responsibilities.

2. Data Protection Principles

This policy is produced according to the principles of data protection as set out in the Data Protection Act (2018) which are in summary:

- Data held and used must be 'fair' and legal
- Data obtained will only be used for specified purpose(s) and will only be used in ways that are compatible with the purposes
- Data must be adequate, relevant & not excessive
- Data must be accurate & up to date
- Data must not be held longer than necessary
- Data Subjects' rights must be respected
- Data will be held with the appropriate level of security
- Special rules apply to transfers abroad.

This policy applies to information relating to identifiable individuals, even where it is technically outside the scope of the Data Protection Act, by virtue of not meeting the strict definition of 'data' in the Act.

3. Policy Statement

EIA UK will:

- comply with both the law and good practice
- respect individuals' rights
- be open and honest with individuals whose data is held
- provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently.

EIA UK recognises that its first priority under the Data Protection Act is to avoid causing harm to individuals.

In the main this means:

- keeping information securely in the right hands, and
- holding good quality information.

Secondly, the Act aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, EIA UK will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

4. Key Risks

EIA UK has identified the following potential key risks, which this policy is designed to address:

- Breach of confidentiality (information being given out inappropriately)
- Insufficient clarity about the range of uses to which data will be put, leading to Data Subjects being insufficiently informed
- Failure to offer choice about data use when appropriate
- Breach of security by allowing unauthorised access
- Failure to establish efficient systems of managing for ensuring that personal data being not up to date
- Harm to individuals if personal data is not up to date
- Insufficient clarity about the way personal data is being used
- Failure to offer choices about use of contact details for staff, volunteers or consultants working for EIA UK
- Data Processor contracts

5. Directors / Trustees responsibility

The Directors / Trustees of EIA UK recognise their overall responsibility for ensuring that EIA UK complies with its legal obligations.

6. Data Protection Officer

The Data Protection Officer is currently the Head of Operations, with the following responsibilities:

- Briefing the Senior Management Team on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Notification
- Handling subject access requests
- Approving unusual or controversial disclosures of personal data
- Approving contracts with Data Processors

7. Line Managers / Team responsibility

Every team or department where personal data is handled is responsible for drawing up its own operational procedures to ensure that good Data Protection practice is established and followed.

8. Staff, Volunteers and Consultants

All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data that they may handle in the course of their work.

9. Breaches of policy

Significant breaches of this policy will be handled under EIA UK's disciplinary procedures.

10. Confidentiality

Because confidentiality applies to a much wider range of information than Data Protection, EIA UK has a separate Confidentiality Policy. Staff, volunteers and consultants are required to sign a short statement indicating that they have been made aware of their confidentiality responsibilities.

11. Privacy Statement

EIA UK has a privacy statement for Data Subjects, setting out how their information will be used. This is available on request, and a version of this privacy statement is on the EIA UK website.

12. Authorisation for Disclosure

Where anyone within EIA UK feels that it would be appropriate to disclose information in a way contrary to the confidentiality policy, or where an official disclosure request is received, this will only be done with the authorisation of the Data Protection Officer. All such disclosures will be documented.

13. Security

This refers to security issues relating to personal data. It does not cover security of the building, business continuity or any other aspect of security.

EIA UK has identified the following risks:

- Information passing between the UK office and mailing houses could go astray or be misdirected.
- Staff or volunteers with access to personal information could misuse it.
- Consultants or volunteers could continue to be sent information after they have stopped working for EIA UK, if their records are not updated promptly.
- Poor web site security might give a means of access to information about individuals once individual details are made accessible on line.
- Staff may be tricked into giving away information, either about supporters or colleagues, especially over the phone or via emails

14. Security Levels

Information held on EIA UK's server is controlled by variable access to folders and files and the supporter's database is password protected.

15. Database

EIA UK has a single fundraising database holding basic information about all supporters.

EIA UK will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

- ICT systems will be designed, where possible, to encourage and facilitate the entry of accurate data.
- Data on any individual will be held in as few places as necessary, and all staff and volunteers will be discouraged from establishing unnecessary additional data sets.
- Effective procedures will be in place so that all relevant systems are updated when information about any individual changes.
- Staff or volunteers who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping.

16. Updating and checking

EIA UK will carry out a partial check of the information held on the fundraising database annually and a complete check every 3 years.

17. Date of last review: May 2018