LAST UPDATED June 11, 2018

DATA PROTECTION POLICY

International Foundation for Electoral Systems

1. Purpose

1.1. International Foundation for Electoral Systems is committed to complying with privacy and data protection laws including:

1.1.1. The Regulation (EU) 2016/679 of the European Parliament (“General Data Protection Regulation” and/or "the GDPR") and any related legislation which applies in the EU, including, without limitation, any legislation derived from the Data Protection Bill 2017;

1.1.2. The Privacy and Electronic Communications Regulations (2003) and any successor or related legislation, including without limitation, E-Privacy Regulation 2017/0003; and

1.1.3. All other applicable laws and regulations relating to the processing of personal data and privacy, including statutory instruments or any other supervisory authority.

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 International Foundation for Electoral Systems 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. Scope

2.1. The types of personal data that we may handle include details of: Employees, Consultants, Contractors, Donors, and Social Media followers.

2.2. The IT Director at International Foundation for Electoral Systems 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 Richard Twigg who can be contacted at rtwigg@ifes.org or at 202-350-6720.

2.3. This Policy does not cover data rendered anonymous or where pseudonyms are used. Data is rendered anonymous if individuals are no longer identifiable or are identifiable only with a disproportionately large expense in time, cost or labor. The use of pseudonyms involves the replacement of names or other identifiers with substitutes, so that identification of individual persons is either impossible or at least rendered considerably more difficult. If data rendered anonymous become no longer anonymous (i.e. individuals are again identifiable), or if pseudonyms are used and the pseudonyms allow identification of individual persons, then this Policy shall apply again.

3. Definitions

3.1. **Consumer** - Any natural person, but excludes any individual acting in his or her capacity as an Employee or Supplier.

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

3.3. **Employee** - means any current, former or prospective employee, temporary worker, intern or other non-permanent employee of IFES or any current or prospective subsidiary or affiliate of IFES. There is a separate privacy policy for employee data

3.4. **Personal Data - A**ny 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.

3.5. **Data Controllers** - People who, or organizations 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 GDPR. International Foundation for Electoral Systems is the data controller of all personal data that we manage in connection with our work and activities.

3.6. **Data Processors** - 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 organizations such as website hosts, fulfilment houses or other service providers which handle personal data on our behalf.

3.6.1. Processing is any activity that involves use of personal data, whether or not by automated means. It includes but is not limited to:

3.6.2. Collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, disclosing by transmission, disseminating or otherwise making available, restricting, erasing or destruction of personal data.

3.7. **Sensitive Personal Data -** includes information about a person's:

3.7.1. Racial or ethnic origin, political opinions, religious, philosophical or similar beliefs, trade union membership, physical or mental health or condition, sexual life or orientation, genetic data, or biometric data.

3.8. **Supplier** - means any supplier, vendor or other third party (including independent contractor) that provides services or products to IFES.

4. Data Protection Principles

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

4.2. Personal Data should be:

4.2.1. Process fairly, lawfully and transparently

4.2.2. Collected for specified, explicit and legitimate purposes and not further processed in a way which is incompatible with those purposes

4.2.3. Adequate, relevant and limited to what is necessary for the purpose for which it is held

4.2.4. Not kept longer than necessary

4.2.5. 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, when 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:

5.2.1. The type of information we will be collecting (categories of personal data concerned)

5.2.2. Who will be holding their information, i.e. International Foundation for Electoral Systems including contact details and the contact details to the IT Director

5.2.3. 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

5.2.4. The legal basis for collecting their information (for example, are we relying on their consent, as part of a contract between the parties, or on our legitimate interests or on another legal basis

5.2.5. If we are relying on legitimate interests as a basis for processing what those legitimate interests are

5.2.6. 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

5.2.7. 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

5.2.8. details of people or organizations with whom we will be sharing their personal data

5.2.9. if relevant, the fact that we will be transferring their personal data outside the organization and details of relevant safeguards

5.2.10. 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 her self, we must provide that individual with the following information in addition to that listed under 5.2 above

5.3.1. The categories of personal data that we hold

5.3.2. 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 EU and, the right to withdraw consent to the processing of their personal data.

5.5. This fair processing information may be provided in numerous 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 organizations for marketing purposes, without first getting the individual's consent.

7. Personal data should be adequate and accurate

7.1. 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 Director of IT.

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 Director of IT.

9. Rights of individuals under the GDPR

9.1. The GDPR gives people rights in relation to how organizations process their personal data. Everyone who holds personal data on behalf of International Foundation for Electoral Systems needs to be aware of these rights. They include (but are not limited to) the right:

9.1.1. to request a copy of any personal data that we hold about them (as data 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;

9.1.2. to be told, where any information is not collected from the person directly, any available information as to the source of the information;

9.1.3. to be told of the existence of automated decision-making;

9.1.4. to object to the processing of data where the processing is based on either the conditions of public interest or legitimate interests;

9.1.5. to have all personal data erased (the right to be forgotten) unless certain limited conditions apply;

9.1.6. to restrict processing where the individual has objected to the processing;

9.1.7. to have inaccurate data amended or destroyed; and

9.1.8. to prevent processing that is likely to cause unwarranted substantial damage or distress to themselves or anyone else.

10. Types of Data Collected

10.1. Personal Data relating to Consumers may include:

Contact information, such as name, job title, company, postal address, email address and telephone number; and Personal Data in content Consumers provide on our website and other data collected automatically through the website (such as IP addresses, browser characteristics, device characteristics, operating system, language preferences, referring URLs, information on actions taken on our website, and dates and times of website visits).

10.2. Personal Data relating to Suppliers may include:

Contact information, such as name, job title, company, postal address, email address and telephone number, tax identification number, bank account information, information required for us to perform due diligence, background checks, health and safety-related reports, testing, and certifications required by law to perform services; and Personal Data in content Suppliers provide on our website and other data collected automatically through the website (such as IP addresses, browser characteristics, device characteristics, operating system, language preferences, referring URLs, information on actions taken on our website, and dates and times of website visits).

11. Data Security

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

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

11.3. 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.

11.4. 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.

11.5. The following security procedures and monitoring processes must be followed in relation to all personal data processed by us:

11.5.1. Encryption of personal data

11.5.2. Measures to restore availability and access to data in a timely manner in event of physical or technical incident;

11.5.3. Process for regularly testing, assessing and evaluating effectiveness of security measures;

11.5.4. 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);

11.5.5. Entry controls (any stranger seen in entry-controlled areas should be reported);

11.5.6. 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;

11.5.7. Personal data must always be transferred in a secure manner (the degree of security required will depend on the nature of the data - the more sensitive and confidential the data, the more stringent the security measures should be) other measures to ensure confidentiality, integrity, availability and resilience of processing systems;

11.5.8. 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.

12. Transferring Data Including Transfers Outside of the EU

12.1. The GDPR requires that when organizations transfer personal data outside the EU, they take steps to ensure that the data is properly protected. We may transfer personal data outside the EU to entities in the United States of America in the following circumstances: Confidential information for travel logistics, background checks for employment or consultant verification, medical, performance.

12.2. Other Third Parties: We may be required to disclose certain Personal Data to other third parties: (i) As a matter of law (e.g. to tax and social security authorities); (ii) to protect Our legal rights; (iii) in an emergency where the health or security of an employee is endangered (e.g. a fire); (iv) to Law Enforcement Authorities in accordance with the relevant legislation in the different EEA Member States.

12.3. NOTE: The European Commission has determined that the United States of America (USA) does not have an adequate level of data protection as defined in Article 45 of the GDPR. The United States of America does not require entities to have the same level of data protection and the European Union. Additionally, the USA provides limited recourse in the event of a unauthorized disclosure

12.4. For more information, please speak to the IT Director.

13. Processing sensitive personal data

13.1. 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 3.5.

13.2. Purely financial information is not technically defined as sensitive personal data by the GDPR. However, care should be taken when processing such data, as the EU will treat a breach relating to financial data very seriously.

13.3. 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.

13.4. It is not always necessary to obtain explicit consent. There are a limited number of other circumstances in which the GDPR permits organizations 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 Director of IT.

14. Notification

14.1. We will report breaches (other than those which are unlikely to be a risk to individuals) to the EU 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.

15. Monitoring and review of the policy

15.1. This policy is reviewed annually by our Policy Working Group to ensure that it is achieving its objectives.

16. Obligations toward Data Protection Authorities

16.1. We will respond diligently and appropriately to requests from Data Protection Authorities (“DPAs”) about this Policy or compliance with applicable data protection privacy laws and regulations. Employees who receive such requests should contact the Director of Information Technology. We will, upon request, provide DPAs with names and contact details of relevant persons. With regard to transfers of Personal Data between IFES entities, the importing and exporting IFES entities will (i) cooperate with inquiries from the DPA responsible for the entity exporting the data and (ii) respect its decisions, consistent with applicable law and due process rights. With regard to transfers of data to third entities, we will comply with DPAs’ decisions relating to it and cooperate with all DPAs in accordance with applicable legislation.