Date Protection Policy

Reviewed on: May 2024

Next review due: May 2025

Signed: Isaak Kohn

Position: Trustee

Data Protection Policy

PURPOSE OF THE POLICY

1.1. Ozer Umagen is committed to processing data in accordance with the current legislation, which includes:

1. The General Data Protection Regulation (GDPR) and the Data Protection Bill 2017;
2. The Privacy and Electronic Communications Regulation 2003 and E-Privacy Regulation 2017/0003, and related as well as successor regulations, and
3. Any other applicable laws and regulations, including guidance and code of conduct issued by the Information Commissioner's Office (ICO)

3.1. This policy sets out what we do to protect individuals' personal data.

3.2. Anyone who handles personal data in any way on behalf of Ozer Umagen must comply with this policy. Any breach of this policy will be taken seriously and may result in disciplinary action or more serious sanctions.

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

POLICY

2.1 This policy applies to all personal data processed by Ozer Umagen

2.2 Ozer Umagen handles the following personal data:

a. Users' records
b. Donor CRM
c. Volunteers details

2.3 Ozer Umagen is responsible for compliance with data protection regulations and this policy.

2.4 This policy should be reviewed annually by the Trustees of Ozer Umagen.

2.5 Ozer Umagen is registered with the Information Commissioner's Office as an organisation that processes personal data. Our registration number is 106675.

DATA PROTECTION PRINCIPLES

3.1 When processing personal data Ozer Umagen is committed to comply with the six data protection principles set out in the GDPR:

3.2 Article 5 of the GDPR requires that personal data shall 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.

LAWFUL, FAIR AND TRANSPARENT PROCESSING

4.1 Personal data will be obtained in lawful manner for example as legal requirement, through contract, vital interest, public task or active consent.

4.2 When collecting personal data from an individual we will inform that individual:

a. What data we collect;
b. Who will hold the information;
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 data (for example their consent or legitimate interest)
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 data outside the EEA and details of relevant safeguards;
j. the existence of any automated decision-making including profiling in relation to that personal data.

4.3 Where we obtain personal data about a person from a source other than that individual we will provide that individual with the following information in addition to that listed under 4.2 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.

4.4 We will inform individuals of their right to lodge a complaint with the regulator (ICO) and the right to withdraw consent.

4.5 Concise, transparent, intelligible and easily accessible information about data processing will be provide on consent forms, website, mailings and CRM.

PROCESSING DATA FOR THE ORIGINAL PURPOSE

5.1 We will process data for the original purpose the individual was told about when data collected.

5.2 If we need to change the purpose of processing data form the original one, we will seek the individual's consent.

DATA MINIMISATION AND ACCURACY

6.1 We shall ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6.2 We shall take reasonable steps to ensure personal data is accurate.

6.3 Where necessary for the lawful basis on which data is processed, reasonable steps shall be put in place to ensure that personal data is kept up to date. Any out-of-date or inaccurate personal data should be destroyed securely.

RETENTION, ARCHIVING AND REMOVAL

7.1 We will not keep personal data for longer than we need to for the purpose it was collected for.

7.2 The personal data that we hold should be or anonymized or destroyed, erased from our systems when it is no longer needed

RIGHTS OF INDIVIDUALS

8.1 Under the GDPR individual's rights in relation to their personal data include (but are not limited):

a. To request a copy of personal data held, in a portable format;
b. When information gathered not directly from the individual to be told the source of the information
c. To be informed about the existence of any automated decision-making
d. To object to the processing of data when based on public interest or legitimate interest
e. The right to be forgotten (have data erased)
f. To restrict or prevent processing
g. To have inaccurate data amended or destroyed

8.2 Individuals who wish to obtain a copy of their personal data held by Ozer Umagen need to put their request in writing and include:

a. Full name and contact details of the person making the request
b. Relationship to our Charity (staff, trustees, service user etc).

8.3 A proof of identity will be requested before a copy of data is released. We will respond to data access request as soon as possible, or within one calendar month.

8.4 Requests which are reasonable will be processed free of charge. If a request is manifestly unfounded or excessive we may charge a reasonable fee for the administrative costs of complying with the request.

SECURITY

9.1 We keep any personal data secure.

9.2 We have procedure in place to keep data secure. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information, against accidental loss, destruction or damage.

9.3 When personal data is deleted this should be done safely such that the data is irrecoverable.

9.4 Appropriate back-up and disaster recovery solutions shall be in place.

9.5 When we are dealing with sensitive personal data (data on an individual's health, race or sexuality), more rigorous security measures will be implemented for instance, anonymisation or encryption.

9.6 To decide on a need for enhanced security measures we will assess whether the information is sensitive or highly confidential and how much damage could be caused if it fell into the wrong hands.

9.7 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; 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; 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.

INFORMATION SHARING

10.1 We will obtain individuals' consent and explain to them when we are required to receive and share personal data from or with other organisations.

10.2 Where we are required to implement formal data sharing arrangements we will:

a. Stipulate when information can be shared;
b. Specify what security measures need to be in place;
c. Specify who is allowed to authorise data sharing;
d. Require records of sharing to be maintained; and
e. Ensure requirements for dealing with subject access requests.

10.3 We will establish formal agreements with organisations where we are required to share information. We will determine how the information will be processed over its lifecycle, including how it is disposed of.

10.4 We will review these agreements regularly and ensure they continue to meet the Services requirements.

TRANSFERRING DATA OUTSIDE THE EEA

11.1 If we were to transfer personal data to other countries outside the EEA (or one of the countries which are not on the approved list as specified by the EC under the GDPR) we would inform individuals and seek their consent for the transfer.

PROCESSING SENSITIVE PERSONAL DATA

a. Sensitive data as defined by the GDPR and summaries in this policy in the Appendix. We will be clear about processing sensitive data, inform individuals about it and seek their explicit consent for processing this type of data.
b. Financial data is not classified as sensitive, but as required by the ICO's regulations we will take special care when processing financial data.

INFORMATION RISKS

c. We will manage information risks (i.e. loss, damage, malicious attack) in a structured way so that Trustees understand the business impact of personal data related risks and manages them effectively.

4. DATA PROTECTION IMPACT ASSESSMENTS

d. Prior to the introduction of any new technology that may have an impact on the processing of the data subject's personal information, Trustees will carry out a data protection impact assessment to ensure that any risks to the information are addressed and controls put in place

RECORDS

e. We shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

i. The name and details of Ozer Umagen, and the person responsible for data protection;
ii. The purposes for which we collect, hold, and processes personal data;
iii. Details of the categories of personal data collected, held, and processed;
iv. Details of how long personal data will be retained; and
v. Descriptions of all technical and organisational measures taken to ensure the security of personal data.

DATA BREACH

f. A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data. This means that a breach is more than just losing personal data.

g. In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, Ozer Umagen shall

promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO within 72 hours of becoming aware of the breach (more information on the ICO website https://ico.org.uk/).

h. Where a breach is likely to result in a high risk to the rights and freedoms of Service Users, staff or volunteers, we must notify those concerned directly.

i. A 'high risk' means the threshold for notifying individuals is higher than for notifying the Information Commissioner's Office (ICO).

j. Following a data breach we will investigate the causes of the breach and evaluate the effectiveness of our response to it. We will take steps to prevent any further incidents of data breach.

MONITORING AND COMPLIANCE

k. Aside from reviewing this policy annually, we will regularly review systems of collecting and storing personal data to ensure through monitoring and review that they are working as intended in practice.

APPENDIX:

Definitions

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 national or resident. All data subjects

have legal rights in relation to their personal data.

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

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. Ozer Umagen is the data controller of all personal data that we manage in connection with our work and activities.

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 or other service providers which handle personal data on our behalf.

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

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

Processing is any activity that involves use of personal data, whether or not by automated means. It includes but is not limited to: collecting, recording, organising, structuring, storing, adapting or altering, retrieving, disclosing by transmission, disseminating or otherwise making available, alignment or combination, restricting, erasing or destruction of personal data.

Sensitive Personal Data (defined as 'special categories of personal data' under the GDPR) includes information about a person's:

i. racial or ethnic origin;

ii. political opinions;

iii. religious, philosophical or similar beliefs;

iv. trade union membership;

v. physical or mental health or condition;

vi. sexual life or orientation;

vii. genetic data;

viii. biometric data; and

ix. such other categories of personal data as may be designated as 'special categories of personal data'· under the Legislation