Eastern Alliance for Safe and Sustainable Transport.

# EASTERN ALLIANCE FOR SAFE AND SUSTAINABLE TRANSPORT (EASST)

# DATA PROTECTION POLICY

## 1. POLICY STATEMENT

**1.1** Our policy is to comply with the requirements of the UK Data Protection Act 1998 and the General Data Protection Regulation (GDPR) to come into force on 25th May 2018. We are committed to upholding the privacy and freedom rights of our supporters, including the right to be forgotten.

**1.2** The purpose of this policy is to:

(a) Set out our responsibilities in observing and upholding UK laws on data protection;

(b) Provide information and guidance to our employees and partners on how to process personal data and ensure that it is used in accordance with our policy on data protection and their responsibilities; and

(c) Provide information and guidance to any data subject on our policy.

**1.3** Under the UK Data Protection Act 1998 and the General Data Protection Regulation to come into force on 25th May 2018, EASST could face a substantial fine and damage to our reputation should we not be compliant. We therefore take our legal responsibilities very seriously.

**1.4** This policy applies directly to our trustees and to all individuals working within EASST as employees or agents.

## 2. WHAT IS PERSONAL DATA?

**2.1** Personal data is any information relating to an identified or identifiable living person, including: location data; IP address; UDIDs (unique device identifiers); and Cookies.

**2.2** Under the GDRP, personal data also includes genetic and biometric data, data on racial or ethnic origin, health, political opinions, spiritual and philosophical beliefs etc.

## 3. ACQUIRING DATA

**3.1** Personal data will only be processed with the **explicit consent** of the subject or if they have a **legitimate interest** in EASST and our work, for example as an EASST

partner, Trustee, or project partner. Parental consent is required for any child using our information services.

**3.2** We will only ever process data for the purposes for which supporters have given their explicit consent and in as much as it is necessary for specified, explicit, and legitimate purposes within the scope of our work.

**3.3** Any individual has the right to object to use of their data as being of legitimate interest at any time. They can do this by emailing or writing to the Data Protection Officer (contact details below). It is the legal obligation of EASST to prove legitimate interest in processing a subject's data.

**3.4** Silence, pre-clicked boxes or inactivity do not constitute consent.

**3.5** Consent cannot be bundled. Separate consent must be given for separate profiling activities.

**3.6** In all circumstances, sign up agreements must be:

(a) Separated from other agreements;

(b) Written in a clear and concise manner what the consent covers, enabling the subject to make an informed decision;

(c) Provided in a way that is not unnecessarily disruptive of the service;

(d) Obtained by a clear, affirmative action such as ticking an empty box or entering an email address.

**3.7** We do not buy or access data from other sources.

**3.8** We do not supplement our supporter data using other sources (e.g. to estimate wealth).

## 4. STORING DATA

**4.1** We will never ask for, or store, data beyond that which is necessary within the scope of our work.

**4.2** Personal data is stored primarily through the online email marketing provider, MailChimp. Mailchimp has a detailed security policy and procedures in place to ensure data is secure and kept safe. All EASST Mailchimp accounts are password protected.

**4.3** Data may also be stored offline in the form of password protected .csv or .xlsx files for ease of accessibility and in case of issues with connectivity.

**4.4** A centralised record will be kept of all data stored offline, including where this is stored.

**4.5** Any person has the right to access the data held on them by EASST. They can do this by emailing or writing to the Data Protection Officer (contact details below).

**4.6** EASST will respond to any request to access data within 1 month of the request being made. Data will be provided free of charge in a commonly used electronic format, if the request is made electronically.

## 5. SHARING DATA

**5.1** We will under no circumstances sell or lease personal data to third parties and we will not share this information unless we have explicit consent or are required to by law.

**5.2** Data will only ever be shared with contractors or project partners with explicit consent of the individual.

**5.3** Data will not be transferred to countries outside the EEA without adequate protection.

**5.4** All staff must inform the Data Protection Officer if they share any data with project partners or contractors. They should include: the means by which the data was shared, the reason the data was shared, and provide evidence of consent.

## 6. REMOVING DATA/ WITHDRAWAL OF CONSENT

**6.1** A person must be able to refuse consent without detriment. There cannot be a penalty for withdrawing consent.

**6.2** Consent must be as easy to withdraw, as it is to give, and by the same method.

(a) All email correspondence will include an unsubscribe link.

(b) Alternatively data subjects can email the Data Protection Officer to revoke subscription.

(c) All data lists will be cleaned (online and offline) on a monthly basis to ensure requests have been met.

**6.3** All lists and records will be updated at least monthly to ensure requests for erasure have been met.

**6.4** If data has been shared with project partners or contractors, they will be notified in writing immediately to erase this data.

## 7. DATA BREACHES

**7.1** A personal data breach is not only data theft. It is anything that leads to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data where there is a 'risk to the rights and freedoms of individuals'. That is, the breach is likely to result in significant detrimental effect on individuals – such as identity theft or damage to reputation.

**7.2** In the event of a data breach, EASST will inform the Information Commissioner's Office and data subjects involved within 72 hours of any breach being discovered.

## 8. MONITORING & REVIEW

**8.1** All data lists will be cleaned (online and offline) on a monthly basis by the Data Protection Officer.

**8.2** The centralised log will be reviewed monthly by the Data Protection Officer to ensure that it is up to date.

**8.3** An annual data audit will be conducted by the Data Protection Officer to ensure all data held meets GDRP guidelines.

**8.4** EASST Trustees will review the Data Protection Policy annually to ensure its meets GDPR guidelines.

### Data Protection Officer contact details

The Data Protection Officer for EASST is Corrine Vibert
Email: corrine@easst.co.uk

### Other policies and documents

- EASST Privacy Policy
- Terms and Conditions