

Data Protection Policy

Purpose

Refugee Support Europe (RSE) is committed to safeguarding the personal data of our members, donors, staff, volunteers and partners. We comply with:

- UK General Data Protection Regulation (UK GDPR)
- The General Data Protection Regulation (Regulation (EU) 2016/679) (EU GDPR)
- The Data Protection Act 2018 (DPA)
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)
- The Data (Use and Access) Act 2025 (DUAA)

Scope

This policy applies to:

- All staff, trustees, volunteers, contractors, and partners
- All personal data processed by the Charity in the UK, EU or elsewhere
- All systems, physical or digital, used for storing or processing personal data

Definitions

- Personal Data: Any information relating to an identified or identifiable natural person
- Special Category Data: Sensitive data including health, ethnicity, religion, sexual orientation, etc.
- Processing: Any action taken with data (e.g., collecting, storing, using, deleting)
- Data Subject: An individual whose data is being processed.
- Data Controller: RSE, which determines the purposes and means of processing
- Data Processor: RSE, which also conducts the processing data

Lawful Bases for Processing

RSE processes personal data under one or more lawful bases:

- Consent
- Contractual necessity
- Legal obligation
- Vital interests
- Public task
- Legitimate interests (balanced against individual rights)

For marketing and communications (under PECR), we obtain clear opt-in consent where required.

Principles of Data Protection

Under the UK GDPR, EU GDPR and DPA, we commit to processing personal data in accordance with the following principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

Rights of Individuals

We uphold the following rights for data subjects under UK GDPR and EU GDPR:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure ('right to be forgotten')
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision-making and profiling

Under the DUAA, we also enable:

- Right to restrict data reuse across public and private platforms
- Right to understand algorithmic impacts
- Right to opt out of non-essential data access under secondary purposes

Data Collection and Use

We collect data:

- To deliver our charitable services
- For fundraising and communication (subject to consent under PECR)
- To comply with legal or regulatory obligations
- To manage staff, volunteers, and supporters

We ensure data is collected fairly and stored securely.

Data Sharing and Transfers

We only share personal data:

- With third parties under data processing agreements
- With legal authorities when required

- With consent of the data subject

International transfers are conducted in accordance with: [?](#)

- UK GDPR adequacy decisions or safeguards (e.g., SCCs)
- EU GDPR requirements for cross-border data flows
- DUAA principles for domestic and extraterritorial data access limitations

Privacy Policy

Our full Privacy Policy is available on the [Professional Standards](#) page of our website. In brief, we collect and process personal data:

- To provide support services to our members
- To communicate with supporters and donors
- To manage staff and volunteers

Subject Access Requests (SARs)

Anyone has the right to access their personal data held by RSE. Requests should be made in writing as outlined in our Privacy Policy. In addition to access, individuals can also request:

- That we correct any inaccurate data we hold
- That we delete their data, where there is no legal reason for us to retain it
- That we restrict certain types of data processing

We review all such requests in line with UK GDPR and respond within one month.

Security of Personal Data

We implement:

- Physical controls (e.g., secure filing systems)
- Technical controls (e.g., encryption, secure servers, MFA)
- Organisational controls (e.g., training, policies, audits)

Data breaches are managed in line with our Data Breach Response Procedure and reported to the ICO within 72 hours, where required.

Data Breach Response Procedure

RSE is registered with the Information Commissioner's Office (ICO) in line with our obligations under UK data protection law.

If a personal data breach is suspected:

- It must be reported immediately to the Data Protection Lead
- We will assess the breach, contain it and keep a record
- If there is a risk to individuals' rights and freedoms, we will notify the ICO within 72 hours

- Affected individuals will also be informed if required

Retention and Disposal

Data is retained only for as long as necessary. Our Data Retention Schedule outlines specific timeframes. Secure disposal methods (shredding, deletion, degaussing) are used.

Data Retention Schedule

RSE only retains personal data for as long as necessary for the purpose it was collected. We regularly review the data we hold and securely delete or anonymise information that is no longer needed. Retention periods are based on legal obligations, safeguarding requirements and operational needs.

- Records of our service users are kept for two years after last contact, to allow for re-engagement and safeguarding review
- Donor details and donation records are kept for six years to meet financial and tax reporting obligations
- Staff and volunteer records are retained for six years after leaving, in line with employment law

Marketing Communications (PECR Compliance)

- We use opt-in mechanisms for electronic marketing.
- Individuals can withdraw consent at any time.
- Soft opt-in may apply to existing supporters under PECR.
- All emails include clear unsubscribe options.

Training and Awareness

All staff and volunteers receive mandatory data protection training at induction and regular refreshers. Data protection is embedded in all operations and governance.

Accountability and Governance

- A Data Protection Officer (DPO) is appointed (if required under GDPR)
- Data Protection Impact Assessments (DPIAs) are conducted for high-risk processing
- Regular audits ensure compliance with data protection standards and DUAA obligations

Review and Updates

This policy will be reviewed annually or when relevant legislation changes, including updates to the DUAA or international data flow regulations.