UMAY PREVENTION CIC

Data Protection & Processing Policy

Policy Version	1.1
Date of Implementation	15.10.2026
Approved By	Sinem Aksay, Pinar Cangir, Yunus Emre Berk
Date of Approval	15.10.2026
Next Review Date	15.10.2027

1. Policy Statement

Umay Prevention CIC ("UMAY") is committed to protecting the privacy, confidentiality, and security of all personal data entrusted to us. As an organisation supporting women and girls affected by violence and abuse, we recognise the heightened sensitivity of the information we handle and the potential risks associated with its misuse or unauthorised disclosure.

This policy establishes the framework through which UMAY ensures that personal data is processed lawfully, fairly, and transparently. It outlines our responsibilities in safeguarding information relating to service users, staff, volunteers, directors, partners, and stakeholders. The organisation adopts a survivor-centred and trauma-informed approach to data protection, ensuring that individuals' rights and safety remain paramount in all data processing activities.

2. Legal and Regulatory Framework

UMAY processes personal data in accordance with the following legislation and regulatory guidance:

- UK General Data Protection Regulation
- Data Protection Act 2018
- Information Commissioner's Office (ICO) guidance
- Human Rights Act 1998

These frameworks set out the standards for the lawful processing, storage, sharing, and retention of personal data. UMAY adheres to these requirements and implements best practice to ensure compliance. UMAY will register with the ICO and pay the annual data protection fee by Direct Debit from UMAY’s bank account.

3. Scope

This policy applies to all individuals who process personal data on behalf of UMAY, including:

- Directors.
- Employees (permanent, temporary, and sessional)
- Volunteers and interns
- Contractors and consultants
- Partner organisations handling data on UMAY's behalf

The policy covers all forms of personal data, whether held electronically, on paper, or through other media.

4. Definitions

Personal Data: Any information relating to an identified or identifiable individual, such as name, address, contact details, or identification numbers.

Special Category Data: More sensitive information requiring additional protection, including data relating to health, racial or ethnic origin, religion, sexual orientation, or experiences of violence.

Processing: Any operation performed on personal data, including collection, storage, use, sharing, or deletion.

Data Subject: The individual to whom the personal data relates.

Data Controller: Umay Prevention CIC acts as the data controller, determining the purposes and means of processing personal data.

Data Processor: A third party that processes personal data on behalf of UMAY.

5. Data Protection Principles

UMAY adheres to the seven principles of the UK GDPR. Personal data will be:

- Processed lawfully, fairly, and transparently
- Collected for specified, explicit, and legitimate purposes
- Adequate, relevant, and limited to what is necessary
- Accurate and kept up to date
- Kept for no longer than necessary
- Processed securely
- Accountable

6. Lawful Bases for Processing

UMAY identifies an appropriate lawful basis before processing personal data. The most common lawful bases used include:

- Consent: Where individuals have given clear permission.
- Contract: Where processing is necessary to fulfil a contract.
- Legal Obligation: Where processing is required by law.
- Vital Interests: Where necessary to protect someone's life.
- Public Task: Where processing supports activities in the public interest.
- Legitimate Interests: Where processing is necessary for organisational purposes and does not override individuals' rights.

For special category data, UMAY relies on additional conditions such as explicit consent, safeguarding, provision of health or social care, or substantial public interest, particularly in relation to supporting survivors of abuse.

7. Roles and Responsibilities

7.1 Directors

The directors hold overall accountability for ensuring that UMAY complies with data protection legislation and that adequate resources are in place to support effective data governance.

7.2 Data Protection Lead

UMAY's Data Protection Lead is Yunus Emre Berk, Director. The Data Protection Lead is responsible for overseeing compliance, advising staff and volunteers, managing data breaches, and acting as the primary point of contact with the ICO.

7.3 Staff and Volunteers

All staff and volunteers are responsible for handling personal data in accordance with this policy, maintaining confidentiality, and reporting any suspected breaches promptly.

8. Collection and Use of Personal Data

UMAY collects personal data necessary to deliver its services and fulfil organisational functions. This may include:

- Service Users: Contact details, demographic information, risk assessments, case notes, safeguarding information, and support needs.
- Staff and Volunteers: Employment records, payroll information, training records, and emergency contact details.
- Directors and Partners: Contact and governance-related information.
- Supporters and Donors: Contact and communication preferences.

Individuals are provided with privacy notices explaining how their data is collected, used, stored, and shared. Participant forms, on paper and online, include a short privacy notice and a link to the full privacy information on UMAY's website.

9. Information Sharing

Information sharing is undertaken responsibly and only when necessary. UMAY may share personal data with statutory agencies, safeguarding partners, or commissioned service providers where:

- The individual has provided consent;
- There is a legal obligation;
- It is necessary to safeguard a child or vulnerable adult; or
- It is required to prevent serious harm or crime.

Data sharing agreements will be established with partner organisations where appropriate to ensure compliance and accountability.

10. Data Security

UMAY implements robust technical and organisational measures to protect personal data against unauthorised access, loss, or misuse. These measures include:

- Secure, password-protected electronic systems.
- Encryption of sensitive data and portable devices.
- Restricted access based on role.
- Secure storage of paper records in locked cabinets.
- Confidential disposal of records through shredding.
- Regular staff training on information security.

11. Data Retention and Disposal

Personal data will be retained only for as long as necessary to fulfil the purposes for which it was collected and to meet legal, regulatory, and safeguarding obligations. UMAY maintains a Data Retention Schedule outlining specific retention periods for different categories of data.

When data is no longer required, it will be disposed of securely, ensuring that confidentiality is maintained.

12. Data Subject Rights

Under the UK GDPR, individuals have the following rights:

- The right to be informed
- The right of access (Subject Access Request)
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights related to automated decision-making and profiling

Requests to exercise these rights should be submitted to the Data Protection Lead and will be responded to within one month, in accordance with legal requirements.

13. Data Breaches

A personal data breach is any incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. All suspected breaches must be reported immediately to the Data Protection Lead.

Where a breach is likely to result in a risk to individuals' rights and freedoms, UMAY will notify the Information Commissioner's Office within 72 hours and inform affected individuals when required. A record of all breaches, regardless of severity, will be maintained.

14. Training and Awareness

UMAY is committed to ensuring that all staff, volunteers, and directors understand their data protection responsibilities. Induction training will be provided, followed by regular refresher sessions and updates when legislative or organisational changes occur.

15. International Data Transfers

UMAY does not routinely transfer personal data outside the United Kingdom. Where such transfers become necessary, appropriate safeguards—such as adequacy regulations or standard contractual clauses—will be implemented to ensure compliance with UK GDPR.

16. Monitoring and Compliance

Compliance with this policy will be monitored through regular internal reviews, audits, and risk assessments. Findings will be reported to the Board of Directors to support continuous improvement and accountability.

17. Related Policies

This policy should be read in conjunction with:

- Privacy Notice
- Safeguarding Policy
- Confidentiality Policy
- Information Sharing Protocol
- Records Retention and Disposal Policy
- Equality, Diversity and Inclusion Policy
- Complaints Procedure

18. Policy Review & Contact

This policy will be reviewed annually or sooner if there are significant legislative or organisational changes. Updates will be approved by the Directors.

For any enquiries, including the execution of your rights regarding this policy should be made via the contact details as shown on the website.