Institute of Domestic Violence, Religion & Migration

Institute of Domestic Violence, Religion & Migration (IDVRM) Data Protection and Management Policy

First drafted on 13 July 2025

Institute of Domestic Violence, Religion & Migration

1. Purpose and Scope

This policy sets out how IDVRM collects, stores, processes, shares and protects personal data in line with:

- The **UK General Data Protection Regulation (UK GDPR)**
- The **EU General Data Protection Regulation (EU GDPR)** (where applicable)
- The **Data Protection Act 2018**
- IDVRM's internal **Research Ethics**, **Safeguarding**, and **Due Diligence Policies**

This policy applies to all IDVRM personnel (paid or unpaid), partners, consultants and collaborators who process personal or sensitive data under IDVRM's affiliation, including in the UK and other international contexts.

2. Core Principles

IDVRM is committed to data protection practices that align with our Core Values, Research Ethics and Safeguarding policies, and these include:

- **Survivor-centred and trauma-informed approaches**
- **Decolonial reflexivity and cultural sensitivity**
- **Transparency, accountability and integrity**
- **Do-no-harm and safeguarding-first principles**

All personal data must be handled according to the following principles:

Principle	Description
Lawfulness, Fairness, and Transparency	Data are processed lawfully, fairly and transparently.
Purpose Limitation	Data are collected for specified, explicit and legitimate purposes only.
Data Minimisation	Only the minimum necessary personal data are collected and processed.
Accuracy	Data are accurate and, where necessary, kept up to date.

Principle	Description
Storage Limitation	Data are retained only for as long as necessary.
Integrity and Confidentiality	Appropriate security measures are in place to prevent misuse or breaches.

3. Legal Bases for Data Processing

IDVRM processes data only when one or more lawful grounds under Article 6 or 9 of the UK/EU GDPR apply. These include:

- **Consent** (freely given, informed, and explicit)
- **Contractual necessity**
- **Legal obligation**
- **Legitimate interests** (balanced against the data subject's rights)
- **Public interest or research purposes**, particularly for safeguarding, violence prevention, and advocacy

Special category data (e.g. relating to religion, ethnicity, health, gender identity, political views) will only be processed:

- With **explicit consent**, or
- Where **necessary for research or safeguarding** in line with Article 9(2)(j) or (g), and with strict protection measures in place

4. Categories of Data Collected

Depending on the nature of the project or engagement, IDVRM may collect:

- **Personal identifiers** (e.g. name, contact info)
- **Demographic data** (e.g. age, gender, nationality, religion, migration status)
- **Health or trauma-related information**
- **Academic or professional background**
- **Audio, visual or written recordings** (e.g. interviews, focus groups)
- **Financial information** (e.g. for honoraria, payroll)

Sensitive personal data will always be handled in compliance with heightened protections and with safeguarding protocols in place.

5. Data Subject Rights

All data subjects have the right to:

- Access their personal data
- Correct inaccurate or incomplete data
- Request erasure (right to be forgotten)
- Restrict or object to processing
- Withdraw consent (where applicable)
- Lodge a complaint with the **Information Commissioner's Office (ICO)** in the UK

Data requests should be sent to the Director or Data Protection Lead if role has been assigned via email.

6. Data Security and Storage

IDVRM ensures secure and ethical data handling through:

- **Password-protected** storage systems (cloud and hardware-based)
- **Encryption** of sensitive datasets and emails containing personal information
- **Access controls** to ensure data is only accessible to authorised team members
- **Secure file transfer** protocols (e.g., encrypted email or trusted platforms)
- **Regular backups** of research data in secure locations
- **Secure deletion protocols** (digital shredding or physical destruction)

7. Retention and Destruction

Data will be retained only for as long as:

- Necessary for the purpose it was collected
- Required by funder or legal obligations
- Needed for research or safeguarding reporting

Data will be **anonymised** or **securely destroyed** after the retention period. Retention schedules will be communicated in consent forms or agreements.

8. Informed Consent and Ethical Use

All research, consultancy and community engagement activities must:

- Follow IDVRM's **Research Ethics Policy**
- Obtain **voluntary, informed, and ongoing consent** in culturally appropriate ways
- Include a **Data Management Plan** approved during the internal ethics review
- Provide **clear privacy notices** explaining data use and rights
- Prioritise **anonymity and safety** in dissemination and publication

Where data are collected from vulnerable populations (e.g. survivors, migrants), researchers must follow **enhanced safeguarding and trauma-informed protocols**.

9. International Data Transfers

IDVRM occasionally works with partners outside the UK/EU. In such cases:

- Data transfers must comply with UK/EU GDPR rules for third-country transfers
- IDVRM will use **appropriate safeguards**, such as:
    - Standard Contractual Clauses (SCCs)
    - Data sharing agreements
    - Country-specific adequacy decisions

Where no adequate safeguards exist, transfers will only take place with **explicit consent** and robust ethical justification.

10. Responsibilities

Role	Responsibility
Director	Oversight of Data Protection and GDPR compliance

Role	Responsibility
Data Protection Lead	Day-to-day data governance, incident response, and training
Researchers and Collaborators	Ensure all data handling complies with this policy and ethical requirements

11. Breaches and Incident Reporting

All data breaches or suspected incidents must be:

- Reported **immediately** to the Director or Data Protection Lead
- Documented and assessed for risk
- Notified to the **ICO** within 72 hours if legally required
- Investigated in line with IDVRM's safeguarding and ethics protocols

IDVRM is committed to **transparency** and will inform affected individuals if their data have been compromised.

12. Training and Capacity Building

IDVRM will:

- Provide GDPR and data ethics training during onboarding
- Offer refresher training on research data management, safeguarding and confidentiality
- Provide guidance on safe communication, consent, and anonymisation in sensitive contexts

13. Review and Updates

This policy will be:

- Reviewed **annually**
- Updated in light of legal changes, new research standards, or lessons learned through implementation
- Re-circulated to all IDVRM team members, partners and collaborators