

DATA PRIVACY & PROTECTION POLICY

Western Solidarity with Ukraine Alliance (WSUA) *Adopted by the Board of Directors*

1. Purpose of This Policy

Western Solidarity with Ukraine Alliance (“WSUA,” “we,” “our,” or “the organization”) is committed to protecting the privacy and personal data of all individuals whose information we collect, including donors, volunteers, beneficiaries, partners, and website users.

This policy ensures compliance with:

- **EU General Data Protection Regulation (GDPR)**
- **Washington State privacy and data protection laws**
- **U.S. nonprofit sector best practices**

WSUA processes personal data lawfully, fairly, transparently, and securely.

2. Scope

This policy applies to:

- All personal data processed by WSUA
- All staff, officers, volunteers, contractors, and partners handling personal data
- All systems, platforms, and tools used to store or process personal data

It covers data collected through:

- Websites
- Donation platforms
- Email communications
- Program activities
- Social enterprise operations
- Events and outreach
- Partnerships and collaborations

3. Definitions (GDPR-Aligned)

Personal Data

Any information relating to an identified or identifiable individual (e.g., name, email, address, IP address, donation history).

Special Category Data

Sensitive data requiring enhanced protection (e.g., health data, political opinions). WSUA does **not** intentionally collect special category data unless necessary for program delivery and with explicit consent.

Processing

Any operation performed on personal data (collection, storage, use, sharing, deletion).

Data Subject

Any individual whose personal data is processed.

Data Controller

WSUA — we determine the purposes and means of processing.

Data Processor

Any third party processing data on our behalf (e.g., payment processors, CRM systems).

4. Legal Basis for Processing (GDPR Article 6)

WSUA processes personal data under the following lawful bases:

4.1 Consent

When individuals voluntarily provide data (e.g., newsletter signup, event registration).

4.2 Contractual Necessity

When data is required to deliver services or fulfill agreements.

4.3 Legal Obligation

Compliance with tax, accounting, or regulatory requirements.

4.4 Legitimate Interests

For mission-aligned activities such as:

- Donor stewardship
- Program administration
- Fraud prevention
- Organizational security

WSUA balances legitimate interests with individual rights.

5. Types of Data We Collect

5.1 Donor Data

- Name
- Contact information
- Donation history
- Payment information (processed securely by third-party processors)

5.2 Volunteer & Staff Data

- Contact information
- Background checks (if required)
- Emergency contacts

5.3 Program Participant Data

- Contact information
- Service delivery records
- Consent forms

5.4 Website & Digital Data

- IP addresses
- Cookies
- Analytics data
- Contact form submissions

5.5 Social Enterprise Data

- Customer information
- Transaction records
- Communications

WSUA does **not** sell personal data.

6. Data Minimization & Purpose Limitation

WSUA collects only the data necessary for:

- Delivering programs
- Managing donations
- Communicating with supporters
- Operating social enterprises
- Complying with legal obligations

Data is not used for purposes incompatible with the original reason for collection.

7. Data Retention

WSUA retains personal data only as long as necessary for:

- Legal compliance
- Program delivery
- Financial reporting
- Donor stewardship

Retention periods follow WSUA's **Document Retention Policy**.

8. Data Security Measures

WSUA implements appropriate technical and organizational measures, including:

- Encrypted storage
- Secure cloud platforms
- Access controls and role-based permissions
- Password protection and MFA
- Staff and volunteer training
- Regular security reviews

Special category data (if collected) receives enhanced protection.

9. Data Sharing & Third-Party Processors

WSUA may share data with trusted third parties such as:

- Payment processors
- Email service providers

- CRM systems
- Cloud storage providers
- Program partners (when necessary)

All processors must:

- Sign data processing agreements (DPAs)
- Comply with GDPR and applicable laws
- Use data only for WSUA-authorized purposes

WSUA does **not** sell or rent personal data.

10. International Data Transfers (GDPR Chapter V)

If personal data is transferred outside the EU/EEA, WSUA ensures:

- Adequacy decisions
- Standard Contractual Clauses (SCCs)
- Appropriate safeguards

WSUA uses reputable, GDPR-compliant service providers.

11. Data Subject Rights (GDPR Articles 12–23)

Individuals have the right to:

- Access their data
- Correct inaccurate data
- Request deletion (“right to be forgotten”)
- Restrict processing
- Object to processing
- Data portability
- Withdraw consent at any time
- Lodge a complaint with a supervisory authority

Requests may be submitted to: **privacy@wsua.org** (or your chosen address)

WSUA will respond within **30 days**.

12. Children's Data

WSUA does not knowingly collect data from children under 16 without parental consent.

13. Data Breach Response

In the event of a data breach:

1. WSUA will assess the scope and impact
2. Contain and mitigate the breach
3. Notify affected individuals when required
4. Notify EU supervisory authorities within **72 hours** if GDPR applies

A breach log will be maintained.

14. Accountability & Governance

WSUA maintains:

- A Data Protection Lead (DPL) — typically the Executive Officer
- Staff training
- Data processing records
- Policies and procedures
- Regular reviews of compliance

15. Policy Review

This policy shall be reviewed every **two years** or upon major legal or operational changes.