

## Data Protection Policy

Approved by BoT on April 10, 2026

### 1. Purpose and scope

This policy defines WECF's commitment to protecting personal data and privacy rights in a manner consistent with the EU General Data Protection Regulation (GDPR), applicable national laws, and the organisation's broader integrity and accountability framework. It applies to all personal data processed by or on behalf of WECF, including within projects and programmes.

This policy applies to:

- employees, interns, volunteers, and contractors;
- partners, funders, suppliers, and network contacts;
- website users, event participants, and newsletter subscribers;
- beneficiaries and other individuals whose data is processed by WECF.

It provides guidance on the management of data collected for the work of WECF.

Technical and organisational security measures are defined in WECF's IT Management and Information Security Policy.

### 2. Accountability and data governance

WECF acts as the Data Controller for personal data processed within its operations. The organisation ensures accountability by embedding data protection within its governance, as part of its Integrity Policies (including the Code of Conduct, Anti-Fraud and Anti-Corruption Policy, Whistleblower Policy, and Child Protection Policy). These integrity policies provide the ethical foundation for transparency, confidentiality, and responsible data handling across the organisation. WECF has designated the Office Coordinator as its Privacy Lead, responsible for overseeing compliance with the GDPR, coordinating data protection practices across the organisation, and acting as the primary contact point for data protection-related matters.

#### 3.1 Roles and responsibilities

- **Privacy lead (Office Coordinator)**  
Responsible for coordinating GDPR compliance, advising management,

maintaining documentation, and serving as contact point for supervisory authorities.

- **Management team**

Ensures organisational compliance, allocates resources, and oversees incident response.

- **Project managers**

Ensure personal data used in projects complies with this policy and donor requirements.

- **All staff**

Responsible for handling personal data in accordance with this policy and reporting incidents.

### 3. Lawful processing principles and legal bases for processing

WECF adheres to the core GDPR principles:

- lawfulness, fairness, transparency;
- purpose limitation and data minimization;
- accuracy of personal data;
- storage limitation;
- integrity and confidentiality;
- accountability and documentation.

WECF processes personal data on the following legal bases:

- **Contractual necessity:** employment contracts, service agreements, and partnership agreements.
- **Legal obligations:** financial reporting, tax obligations, labour law requirements.
- **Legitimate interests:** organisational management, communication with partners and stakeholders. See Annex 1.
- **Consent:** newsletters, event participation, and use of images and videos where required.

## 4. Purpose of data collection and categories of data

WECF is a nonprofit network dedicated to a gender just and healthy planet for all. It's international network consists of over 250 women's and civil society organisations in 70 countries. We believe that a sustainable future and environment needs holistic solutions reflecting the lives of people on the ground. We believe in feminist solutions based on our partners' visions and needs. That is why we work on transformative gender equality and women's human rights in interconnection with climate justice, sustainable energy & chemicals, less toxic waste, safe water & sanitation for all.

To successfully build and maintain this network, WECF processes personal data relevant to:

- employment and HR management;
- project and partner management;
- financial, administrative, and donor reporting;
- communications and outreach;
- safeguarding, accountability, and integrity reporting.

Special categories of data (e.g., health, sensitive protection information) are processed only where strictly required and under enhanced safeguards.

WECF processes the following categories of personal data where necessary:

- **Staff and HR data:** name, contact details, employment contracts, payroll information, performance records, emergency contacts.
- **Partner and contractor data:** names, professional contact details, organisational affiliation, contractual and financial information.
- **Donor and funder contacts:** names, professional contact details, correspondence.
- **Event and programme participants:** names, contact details, affiliation, registration information such as gender, location, or other demographic information. We may use this information anonymously to inform our reporting.
- **Website and communication users:** email addresses, newsletter subscriptions, website and social media analytics data.
- **Safeguarding and integrity reports:** personal information submitted in complaints or reports.
- **Photos and video from WECF events:** documentation from events, trainings, workshops etc for reporting, and for use on WECF's website and social media.

Attendees, visitors, and participants will be informed as thoroughly as possible about any video recordings before and during the event. This will be done, for example, through announcements at the location, in invitations, or via other communication channels. We will explicitly request permission for specific

recordings of clearly recognizable individuals. If someone reaches out to us and wants their photo or video to be removed, we will respect this.

## 5. Data integrity and purpose

Personal data is used only for clearly defined purposes related to organisational functions, legal obligations, programme delivery, donor compliance, and accountability to stakeholders. Data is not retained or repurposed without appropriate legal basis and safeguards.

## 6. Data sharing and contractual controls

Personal data may be shared:

- internally, on a **need-to-know basis**;
- with authorised service providers or processors (with data processing agreements);
- with funders and auditors where required for compliance;
- with partners when necessary for project implementation under contract.

Data sharing with third parties is governed by contractual requirements that include confidentiality and data protection obligations consistent with this policy and GDPR. Before engaging a new service provider that processes personal data, WECF assesses whether appropriate data protection safeguards are in place. Vendors must comply with data protection requirements.

## 7. International data transfers

WECF primarily uses cloud-based collaboration tools for email, document storage, and internal communication. WECF may also use external service providers for functions such as communication and administration. Some of these providers may process personal data outside the EU. In such cases, WECF ensures that appropriate safeguards are in place to protect personal data in accordance with the GDPR. These safeguards include:

- service providers located in countries recognised by the European Commission as providing adequate data protection; or
- contractual safeguards such as Standard Contractual Clauses (SCCs).

Before engaging a new service provider that may process personal data outside the EU/EEA, WECF verifies that appropriate data protection safeguards are in place.

## 8. Safeguarding, security, and integrity integration

WECF's data protection practices are integrated with its IT Security Policy and Integrity Policies to ensure comprehensive safeguarding:

- technical and organisational security measures are applied to protect confidentiality, availability, and integrity of data (role-based access, multi-factor authentication, secure storage, logging and monitoring);
- data protection is embedded in staff onboarding and training, consistent with WECF's Code of Conduct and Anti-Fraud Policy;
- misuse of personal data or breaches of privacy are treated as integrity violations and addressed under existing procedures, including whistleblowing and reporting mechanisms.

## 9. Data breach and incident response

Any suspected or confirmed personal data breach must be reported immediately to the Privacy Lead and Management. WECF will assess the breach, contain risks, record it internally, and notify authorities or affected individuals if required under GDPR. Donors or partners will be informed when contractual obligations demand it.

## 10. Data subject rights

Individuals have the right to:

- access, rectify, or erase their personal data;
- restrict or object to processing;
- data portability;
- withdraw consent where applicable;
- lodge complaints with WECF or a supervisory authority.

Requests may be submitted via [privacy@wecf.org](mailto:privacy@wecf.org).

WECF will verify the identity of the requester, respond within **one month** in accordance with GDPR and coordinate requests with relevant departments where necessary. The Privacy Lead of WECF will handle the requests.

## 11. Data retention and disposal

Personal data is retained no longer than necessary and in accordance with legal and donor requirements. Retention periods are documented and reviewed.

### 11.1 Human resources data

Personal data relating to employees, interns, and contractors (including employment contracts, payroll information, and administrative records) is retained for **7 years** after the end of employment, in accordance with Dutch tax and labour regulations.

Purpose: To manage employment relationships and comply with legal obligations.

### 11.2 Partners, donors and other stakeholders

Personal data of partners, funders, and other stakeholders (such as names, professional contact details, and organisational affiliations) is retained for the duration of the relationship and for a reasonable period thereafter.

Data is reviewed **yearly** and deleted when:

- the relationship is no longer active;
- the individual is no longer affiliated with the partner organisation;
- continued retention is no longer necessary for project, reporting, or accountability purposes.

Purpose: To enable effective collaboration, communication, and implementation of projects and organisational activities, based on WECF's legitimate interest.

### 11.3 Applicants

Personal data of job applicants (such as CVs, motivation letters, and contact details) is retained for the duration of the recruitment process, and for up to **4 weeks** after a final candidate is selected, unless a longer retention period is agreed with an applicant.

Purpose: To manage recruitment processes and assess candidates.

### 11.4 Project data

Personal data contained in project documentation (such as reports, partner information, and supporting documentation) is retained for **10 years** after project completion, in line with EU funding requirements.

Purpose: To ensure compliance with donor obligations, reporting requirements, and accountability.

#### 11.5 Donations and financial data

Personal data related to donations and financial transactions (including donor details and payment records) is retained for **7 years**, in accordance with Dutch tax law.

Purpose: To process donations, maintain financial records, and comply with legal obligations.

#### 11.6 Mailing lists and communication

Personal data used for communication (such as email correspondence, partner contacts, and newsletter lists) is retained for as long as the relationship remains active.

Such data is reviewed **yearly** and deleted when there has been no meaningful contact for a prolonged period; the individual is no longer relevant to WECF's activities; or the individual unsubscribes or requests deletion.

Purpose: To maintain communication with stakeholders and support organisational activities, based on consent or legitimate interest where applicable.

#### 11.8 Third Parties and service providers

Personal data processed by third-party service providers (such as IT systems, newsletter providers, and administrative tools) is retained in accordance with WECF's retention rules and the contractual agreements in place with the provider.

WECF ensures that personal data is not retained longer than necessary, that providers apply appropriate technical and organisational measures, and that data is deleted or anonymised when no longer required.

Purpose: To enable WECF to use external services necessary for its operations while ensuring GDPR-compliant data handling.

## 12. Review and updates

This policy is reviewed periodically to reflect changes in law, organizational practice, or data processing activities. The latest version is published and communicated internally.