

Solvoz Foundation Data Governance and GDPR Role Allocation Framework

Document status: Version 2.0 – October 2026

Applies to: Stichting Solvoz Foundation

Registered office: The Hague, The Netherlands

Address: Biancaland 100, 2591 DB The Hague, The Netherlands

Chamber of Commerce number: 75501325

RSIN: 860304863

1. Purpose

This document establishes the data governance framework and GDPR role allocation principles for Stichting Solvoz Foundation and the programmes, partners and service providers with which it works.

The Foundation may develop, coordinate, fund or participate in programmes involving procurement knowledge, supplier inclusion, market access, sourcing, shared infrastructure, digital tools, research and sector collaboration. Some Foundation-supported programmes may involve the processing of personal data through digital platforms or external service providers.

This framework is intended to ensure that:

- data protection roles are determined according to the actual processing activity;
- responsibilities between the Foundation, participating organisations and service providers are clearly documented;
- personal data is handled in accordance with applicable data protection requirements;
- operational data access is appropriately controlled;
- no technology or service provider is assumed in advance to fulfil a particular GDPR role solely because of a historic or organisational relationship.

This document supports compliance with:

- the EU General Data Protection Regulation (“GDPR”);
- applicable Dutch data protection requirements;
- relevant guidance of the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).

Where one party processes personal data on behalf of another party acting as Controller, the relevant processing relationship must be appropriately documented.

This framework should be read together with the Foundation’s Policy Plan, Governance Charter, Conflict of Interest Policy, Related-Party Transaction Policy, Grant Funding Policy, IP and Open-Access Knowledge Policy and relevant programme or service agreements.

2. Organisational and operational roles

2.1 Solvoz Foundation

Solvöz Foundation exists to support its statutory public-benefit objective, including:

- open-access procurement knowledge;
- responsible and inclusive procurement practices;
- local and regional market access;
- supplier and SME inclusion;
- research and collaboration initiatives;
- market assessments and supplier mapping;
- shared procurement infrastructure and tools;
- capacity strengthening;
- standards and methodologies;
- programme coordination and sector collaboration.

Depending on the nature of a specific programme or processing activity, the Foundation may act as:

- Controller;
- Joint Controller;
- contracting or programme entity without an operational data-processing role;
- or, where legally and operationally appropriate, another role determined by the factual processing arrangement.

The Foundation's GDPR role must therefore be assessed per processing activity or programme and must not be assumed solely on the basis of its organisational status.

2.2 External technology and service providers

The Foundation may work with external technology providers, hosting providers, implementation partners, research organisations, consultants and other service providers where these are required for programme delivery. Such providers may act, depending on the actual arrangement, as:

- Processor;
- Sub-processor;
- independent Controller;
- Joint Controller;
- technology or hosting provider without access to personal data;
- or another role determined by the nature of the processing.

No particular technology or service provider has an automatic, exclusive, preferred or default operational role within Foundation-supported programmes. When an related party is selected for a specific programme, its GDPR role must be assessed and documented, alongside the additional governance requirements of the Foundation's Conflict of Interest Policy and Related-Party Transaction Policy.

3. Governance principles

The following governance principles apply:

- GDPR roles are determined by the actual purposes, means and circumstances of the processing;
- organisational labels alone do not determine Controller or Processor status;
- the Foundation, programme partners and service providers should have clearly documented responsibilities;
- personal data processing roles should be determined per programme or processing activity;
- operational procurement data should remain accessible only to parties that have an authorised operational need;
- appropriate contractual arrangements must exist between Controllers, Processors and other relevant parties;
- data minimisation and least-privilege access principles apply;
- related-party relationships do not override or predetermine data protection role allocation;
- programme and provider selection should be separated from the legal assessment of the resulting data-processing roles.

4. GDPR role allocation principles

4.1 Programme-specific role allocation

There is no single mandatory GDPR role structure for all Foundation-supported programmes. Roles must be determined according to the actual programme and processing activity. A typical procurement or sourcing deployment may, for example, involve:

Entity	Possible GDPR role
NGO / client organisation determining its procurement process	Controller
Foundation	Controller, Joint Controller or no operational processing role, depending on the activity
Technology or platform provider	Processor or other role depending on the processing arrangement
Hosting provider	Processor or Sub-processor, depending on the contractual structure
Programme or research partner	Role determined by its actual processing activities

Where a client or participating organisation independently determines the purpose and essential means of its own procurement-related processing, that organisation will normally have Controller responsibilities for that processing. Where a technology or service provider processes personal data only on documented instructions from a Controller, the relevant Processor requirements apply. Where the Foundation itself determines the purposes and means of a processing activity, the Foundation may act as Controller for that activity. Where two or more

parties jointly determine relevant purposes and means, the possibility of Joint Controllership must be assessed and documented.

4.2 No assumed provider role

The use of a particular technology, platform or service provider does not automatically determine the Foundation's GDPR role or the roles of participating organisations. Role allocation must be based on the actual processing arrangements for the specific programme.

5. Foundation processing activities

The Foundation may independently act as Controller for activities related to its own operations and public-benefit programmes. Typical activities may include:

Activity	Typical GDPR role of Foundation
Foundation administration	Controller
Research collaboration management	Controller
Event registrations	Controller
Mailing lists and communications	Controller
Partnership coordination	Controller
Knowledge-sharing initiatives	Controller
Working groups and governance initiatives	Controller
Standards and methodology development	Controller
Grant and donor management	Controller
Supplier outreach and programme registration	To be assessed according to the specific programme
Programme monitoring and evaluation	To be assessed according to the specific processing

Where the Foundation participates in operational procurement, supplier or programme data processing, its role must be expressly assessed rather than presumed.

6. Operational data access restrictions

Access to operational procurement and programme data must be limited according to role and operational necessity. Foundation board members, staff, researchers, partners, contractors and service providers should not have access to operational data merely because of their organisational relationship with the Foundation. Access to information such as:

- customer procurement records;
- supplier bids;
- tender evaluations;
- operational user accounts;
- confidential supplier information;
- confidential platform transaction data;

must be based on a legitimate operational need and the relevant documented processing arrangement.

Any exceptional or privileged access must:

- be justified;
- be appropriately authorised;
- be documented where required;
- be limited to the necessary scope;
- comply with applicable GDPR and confidentiality requirements.

Access rights should be reviewed and withdrawn when no longer required.

7. Data role assessment requirement

Before a new material programme or deployment involving personal data becomes operational, the relevant parties should document, where applicable:

- the processing activities involved;
- identity of the Controller or Controllers;
- identity of Processor(s);
- any Sub-processor involvement;
- the Foundation's role;
- the role of programme partners;
- hosting arrangements;
- categories of personal data processed;
- relevant data subjects;
- access-control responsibilities;
- data retention responsibilities;
- international or cross-border transfer implications;
- whether any Joint Controllership exists;
- relevant contractual arrangements.

A deployment-specific Data Role Assessment or annex may be created for each material implementation. Existing programmes should be reviewed where their operating model, providers or processing activities materially change.

8. Data Processing Agreements

8.1 Requirement

Where an external provider processes personal data on behalf of a Controller, the appropriate written data-processing arrangements must be in place. A Data Processing Agreement should address, as relevant:

- subject matter and scope of processing;
- duration;
- nature and purpose of processing;
- categories of data and data subjects;
- security obligations;
- confidentiality;
- Sub-processor conditions;
- breach notification responsibilities;

- deletion or return of data;
- audit and information obligations;
- assistance with data subject rights;
- other applicable GDPR requirements.

8.2 Typical relationships

Possible relationships may include:

Controller	Processor
NGO / participating organisation	Selected platform or technology provider
Solvoz Foundation for its own processing activities	Selected external service provider
Programme Controller	Hosting, software or specialist processor

The identity of the Processor is determined per programme. A Data Processing Agreement between the Foundation and a particular provider is required only where that provider processes personal data on behalf of the Foundation acting as Controller.

9. Security and confidentiality

Appropriate technical and organisational measures should be maintained according to the nature, sensitivity and risk of the processing. These may include:

- role-based access controls;
- multi-factor authentication;
- encryption in transit and at rest;
- logging and monitoring;
- vulnerability management;
- secure development practices;
- backup and recovery controls;
- incident-response procedures;
- confidentiality obligations;
- access review and removal procedures.

The specific security responsibilities of the Foundation, participating organisations and service providers should be documented where relevant. Access must be restricted according to operational necessity and least-privilege principles.

10. AI and analytical functionality

Where AI-assisted or analytical functionality is used, including:

- comparative reporting;
- supplier matching;
- bid analysis;
- recommendation systems;
- procurement analytics;

- other automated or assisted analysis;

the relevant Controller remains responsible for its applicable data protection obligations, including lawful processing, appropriate transparency and human oversight where required.

Where an external provider processes personal data on behalf of a Controller in connection with such functionality, that provider must act within the scope of the documented processing arrangement. The Foundation should assess its own role separately where it determines, jointly determines or materially influences the purposes and means of an AI-related processing activity.

11. International data transfers

Where personal data is transferred outside the European Economic Area and a transfer mechanism is required, appropriate lawful safeguards must be used. These may include, where applicable:

- adequacy decisions or mechanisms;
- Standard Contractual Clauses;
- other recognised lawful transfer safeguards.

The relevant Controller and Processor arrangements should document responsibility for international transfers where applicable. Provider selection should take into account applicable data-location, transfer and compliance requirements.

12. Data subject rights

Controllers remain responsible for ensuring that applicable data subject rights can be exercised. These may include, where relevant:

- access;
- rectification;
- deletion;
- restriction;
- portability;
- objection;
- other applicable rights.

Processors must provide the assistance required under the relevant processing arrangement and applicable law. Where more than one organisation is involved in a programme, responsibilities for handling data subject requests should be clearly allocated.

13. Audit and oversight

The governance structure should support:

- clear operational accountability;
- documented GDPR role allocation;
- separation of responsibilities where appropriate;
- controlled access to operational data;
- documented conflict-of-interest management;
- appropriate oversight of service providers;
- periodic compliance reviews;

- reassessment when programmes or provider arrangements materially change.

The board retains oversight of the Foundation's own compliance responsibilities but does not automatically assume operational responsibility for processing performed independently by programme partners or external providers.

14. External providers and related-party arrangements

The Foundation may work with different technology providers, programme partners and specialist service providers depending on the needs of a programme. No external provider has an automatic, exclusive, preferred or default role in the Foundation's data-processing arrangements.

The Foundation's organisational independence and data-governance responsibilities must be maintained irrespective of the provider selected. Where a related party provides technology, hosting, implementation or another service in a specific programme:

- the provider must have been selected in accordance with the Foundation's applicable governance policies;
- its GDPR role must be determined according to the actual processing performed;
- relevant service and data-processing arrangements must be documented;
- access to personal or operational data must be limited to what is necessary;
- the relationship must not create broader data access or governance rights merely because of the related-party relationship.

The Foundation does not direct processing performed independently by another Controller unless such a role has been expressly established through the actual programme and processing arrangements.

15. Recommended supporting documentation

Depending on the programme and processing activities, supporting documentation may include:

1. Deployment- or programme-specific Data Role Assessments
2. Data Processing Agreements
3. Joint Controller arrangements where applicable
4. Sub-processor Registers
5. Access Control documentation
6. Records of Processing Activities (ROPA)
7. Privacy Notices
8. Information Security Policies
9. Incident Response Procedures
10. Conflict of Interest records
11. Related-Party Transaction records where relevant
12. AI Governance and Human Oversight Guidelines where relevant
13. Data retention arrangements
14. International data-transfer documentation where applicable

Documentation should be proportionate to the nature, scale and risk of the relevant processing.

16. Review and approval

This framework should be:

- reviewed at least once every two years;
- updated following material organisational, programme, provider or operational changes;
- reviewed where a material new category of personal-data processing is introduced;
- validated as appropriate before major deployments or significant changes to processing arrangements.

Changes to this framework require board approval.