Solvoz Foundation
Data Governance and GDPR Role Allocation Framework

Document status: Version 1.0 – May 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 governance framework, GDPR role allocation principles, and operational separation between:

- Solvoz Foundation as a non-commercial mission-oriented entity focused on safeguarding knowledge, methodologies, standards, interoperability, and ecosystem stewardship; and
- Solvoz BV as the operational technology provider responsible for development, hosting, support, maintenance, and commercial deployment of procurement technology platforms.

This document supports compliance with:

- the EU General Data Protection Regulation ("GDPR");
- Dutch data protection requirements; and
- guidance issued by the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).

The Dutch supervisory authority states that:

- the controller remains responsible for personal data processing; and
- a written processing agreement must exist where a processor processes personal data on behalf of a controller.

2. Organisational Separation

2.1 Solvoz Foundation

Solvoz Foundation exists to support:

- knowledge safeguarding,
- public-interest governance,
- interoperability principles,
- ecosystem development,
- standards and methodologies,
- ethical procurement practices,
- research and collaboration initiatives,
- and non-commercial stewardship activities.

The Foundation is not intended to act as the operational procurement platform operator for customer deployments unless explicitly agreed in a separate documented arrangement.

2.2 Solvoz BV

Solvoz BV acts as:

- software developer,
- technology provider,
- hosting and infrastructure manager,
- implementation partner,
- support provider,
- and operational platform service provider.

Solvoz BV may process personal data on behalf of customer organisations using procurement and tendering platforms.

3. Governance Principles

The following governance principles apply:

- Clear separation shall exist between Foundation governance functions and commercial operational functions.
- Operational customer data shall remain under the responsibility of the relevant customer organisation and operational service providers.
- Foundation personnel shall not access operational procurement data unless explicitly authorised and documented.
- Personal data processing roles shall be determined per deployment.
- Appropriate contractual arrangements shall exist between controllers and processors.
- Data minimisation and least-privilege access principles shall apply at all times.

4. GDPR Role Allocation Principles

4.1 Standard Operational Deployment Model

In the standard deployment structure, the following GDPR roles apply:

Entity	Typical GDPR Role
NGO / Client Organisation using the platform	Controller
Solvoz BV	Processor
Cloud hosting providers	Sub-processors
Solvoz Foundation	Not involved in operational processing

Under this model:

- the client organisation determines the purpose and means of procurement-related processing;
- Solvoz BV processes personal data solely under customer instructions;
- and the Foundation remains organisationally separate from operational processing activities.

5. Foundation Processing Activities

The Foundation may independently act as Controller for limited internal activities related to its own operations.

5.1 Typical Foundation Processing Activities

Activity	GDPR Role of Foundation
Research collaboration management	Controller
Event registrations	Controller
Mailing lists and communications	Controller
Working groups and governance initiatives	Controller
Knowledge-sharing initiatives	Controller
Partnership coordination	Controller
Standards and methodology development	Controller

These activities are separate from operational procurement platform processing.

6. Operational Data Access Restrictions

Operational procurement platform data shall remain segregated from Foundation activities.

Unless explicitly authorised through documented governance procedures:

- Foundation board members,
- Foundation staff,
- Foundation researchers,
- and Foundation partners

shall not access:

- customer procurement records,
- supplier bids,
- tender evaluations,
- operational user accounts,
- or confidential platform transaction data.

Any exceptional access must:

- be justified,
- documented,
- approved by authorised operational management,
- and comply with GDPR principles.

7. Data Role Assessment Requirement

Prior to any operational deployment, the following must be documented:

- identity of the controller;
- identity of the processor(s);
- hosting arrangements;
- sub-processor involvement;
- cross-border transfer implications;
- access control responsibilities;
- and whether any joint controllership exists.

A deployment-specific annex may be created for each implementation.

8. Data Processing Agreements (DPA)

8.1 Requirement

Where Solvoz BV processes personal data on behalf of a customer organisation acting as Controller, a written Data Processing Agreement must be concluded.

The DPA shall define:

- processing scope,
- duration,
- security obligations,
- confidentiality,
- sub-processor conditions,
- breach notification requirements,
- and data subject rights assistance obligations.

8.2 Typical DPA Relationships

Controller	Processor
NGO / Client Organisation	Solvoz BV
Foundation (for its own operational activities if outsourced)	Service Provider / Processor

The Foundation does not automatically require a DPA with Solvoz BV unless Solvoz BV processes Foundation-controlled personal data on behalf of the Foundation.

9. Security and Confidentiality

Appropriate technical and organisational measures shall be maintained, including:

- role-based access controls,
- MFA authentication,
- encryption in transit and at rest,
- logging and monitoring,
- vulnerability management,
- secure development practices,
- backup and recovery controls,
- and incident response procedures.

Access shall be restricted according to operational necessity.

10. AI and Analytical Functionality

Where AI-assisted functionality is used, including:

- comparative reporting,
- supplier matching,
- bid analysis,
- recommendation systems,
- or procurement analytics,

the operational Controller remains responsible for:

- lawful processing,
- transparency obligations,
- and human oversight requirements.

Solvoz BV shall process such data solely under documented instructions where acting as Processor.

11. International Data Transfers

Where personal data is transferred outside the European Economic Area (EEA), appropriate safeguards shall be implemented, including:

- Standard Contractual Clauses (SCCs),
- adequacy mechanisms,
- or equivalent lawful transfer safeguards.

12. Data Subject Rights

Controllers remain responsible for responding to:

- access requests,
- deletion requests,
- rectification requests,
- portability requests,
- and objections.

Processors shall provide reasonable assistance where contractually required.

13. Audit and Oversight

The governance structure should ensure:

- clear operational accountability;
- separation between governance stewardship and operational processing;
- documented conflict-of-interest management;
- and periodic compliance reviews.

14. Relationship Between Foundation and BV

The relationship between:

- Solvoz Foundation and
- Solvoz BV

is intended to maintain:

- governance independence,
- mission stewardship,
- operational clarity,
- and GDPR role separation.

The Foundation does not direct operational customer data processing unless explicitly defined in a separate documented governance arrangement.

15. Recommended Supporting Documentation

The following supporting documents are recommended:

1. Deployment-specific Data Role Assessments
2. Customer Data Processing Agreements
3. Sub-processor Register

4. Access Control Policy
5. Records of Processing Activities (ROPA)
6. Privacy Notices
7. Information Security Policies
8. Incident Response Procedures
9. Conflict of Interest Policy
10. AI Governance and Human Oversight Guidelines

16. Review and Approval

This framework should be:

- reviewed every two years;
- updated following material organisational or operational changes;
- and validated prior to major deployments or governance changes.