National Federation of
Voluntary Service Providers
Pension & Life Assurance Scheme

Data Governance Framework

July 2026

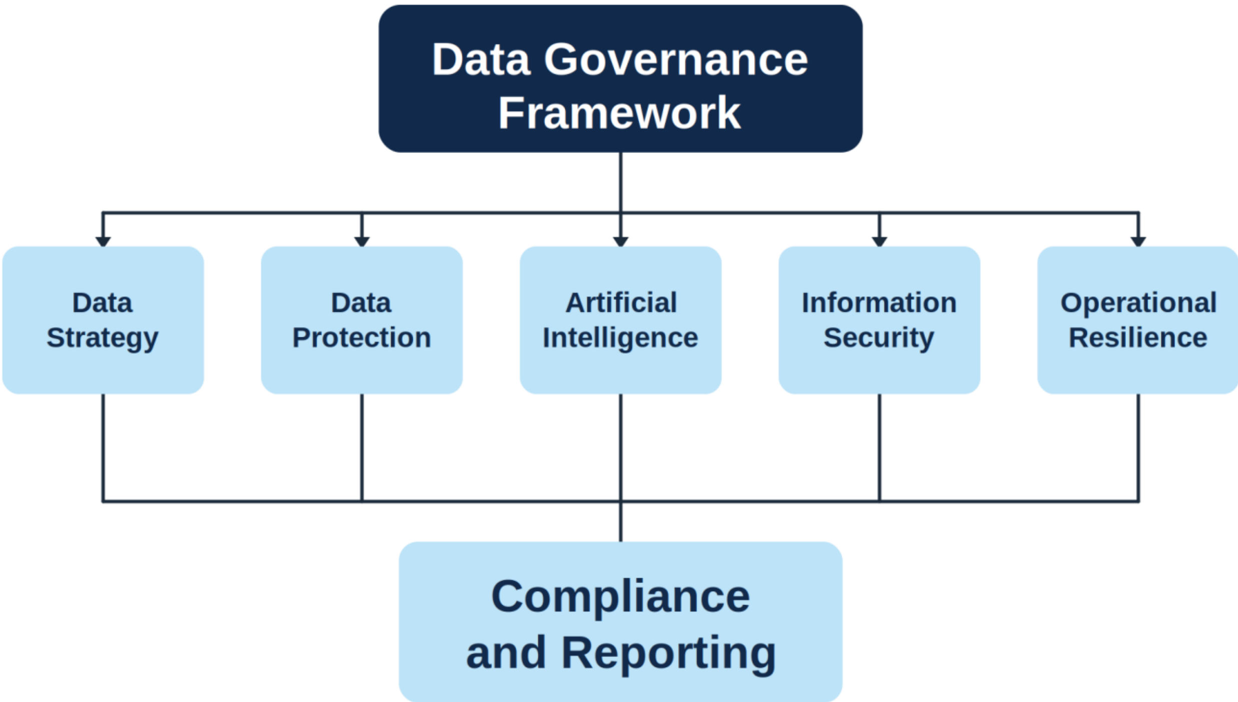
Oranmore Business Park, Oranmore, Galway, Ireland, H91 TP2W.
+ 353 (0)91 792316 pensionadmin@fedvol.ie www.fedvol.ie
Pension Authority No: PB67866 Revenue Approval No: SF7346

1. INTRODUCTION:

This Data Governance Framework provides an overarching structure for the effective management, protection, and utilisation of data within the National Federation's Pension & Life Assurance Scheme (the "Scheme"). It is designed to ensure compliance with relevant regulatory requirements, including the Pensions Authority Code of Practice, the General Data Protection Regulation (GDPR) and the Irish Data Protection Act 2018, the Digital Operational Resilience Act (DORA), and general information security best practices.

This framework establishes the principles, responsibilities, and key areas of focus for data governance, with detailed implementation provided through a suite of supporting policies and procedures.

A diagram showing the principal policies under each pillar and cross-referencing related policies and documents is set out in Appendix 1.



2. PURPOSE OF FRAMEWORK:

The principal aims of this Framework are to ensure relevant Scheme data and information is appropriately maintained to enable the Scheme to:

(a) Meet its objectives, including paying the correct benefits to the correct beneficiary.

(b) Underpin the governance and oversight of the Scheme including regulatory compliance, effective risk management and internal audit.

(c) Provide such reporting as is required, including statutory reporting.

3. FRAMEWORK PRINCIPLES:

This framework is built upon the following core principles:

(a) **Accountability:** Clear assignment of roles and responsibilities for data management.

(b) **Compliance:** Adherence to all applicable legal, regulatory, and ethical obligations.

(c) **Integrity:** Ensuring the accuracy, completeness, and reliability of data.

(d) **Security:** Protecting data from unauthorised access, use, disclosure, alteration, and destruction.

(e) **Transparency:** Openness about data processing activities with data subjects and stakeholders.

(f) **Availability:** Ensuring data is accessible when and where needed for legitimate purposes.

(g) **Value:** Recognising data as a strategic asset that supports the Scheme's objectives.

4. DATA STRATEGY:

Effective data governance requires a clearly defined structure that assigns responsibilities and promotes accountability. The Trustee Board holds ultimate responsibility, supported by key roles such as the Data Protection Team (Pension Scheme Manager and the Professional Trustee) acting as the primary contact for data protection, the participating employers and the Scheme’s administrators and other advisors who act as either Data Controllers or Data Processors. This pillar ensures the accuracy, completeness, and consistency of data throughout its lifecycle, from collection to disposal. It also addresses the specific requirements from the Pensions Authority Code of Practice regarding the information needed for Scheme management.

Supporting Policy and Procedure:

(a) Data Strategy Policy: This policy outlines the overall principles, objectives, roles and responsibilities for data management within the Scheme, details the nature, scope, and timeliness of data required by Trustees to manage the Pension Scheme, including standards, procedures and methods for obtaining and verifying its accuracy, completeness and consistency and incorporates the specific information requirements outlined in the Pensions Authority Code of Practice (paragraphs 13, 14, 15, and 16).

(b) Information Procedure: This procedure sets out how the Trustees are to receive the necessary information in a timely fashion to enable them to manage the Scheme in an efficient and compliant manner.

5. DATA PROTECTION:

This pillar ensures the Scheme's adherence to data protection legislation, primarily the General Data Protection Regulation (GDPR) and the Irish Data Protection Act 2018. It focuses on lawful, fair, and transparent processing of personal data, upholding data subjects' rights, and maintaining accountability throughout the data lifecycle.

Supporting Policies and documents:

(a) Data Protection Policy: This policy details the Scheme's commitment to GDPR principles, lawful bases for processing, retention, data subject rights, and the handling of personal data.

(b) Record of Processing Activity (ROPA): This details the personal data that the Scheme processes, the lawful basis for processing and other key information. The Scheme’s ROPA is set out in Appendices 1 to 4 of the Scheme’s Data Protection Policy.

(c) Data Protection Notice (DPN): This provides transparency to the Scheme’s members about how the Trustees process personal data.

(d) Data Incident Response Procedure: This Procedure outlines the procedures for detecting, assessing, managing and responding to personal data breaches, including regulatory and data subject notification requirements.

(e) Data Retention Policy: The Trustees' high-level approach to retention is set out in the Data Protection Policy with further specific details contained in the Data Retention Policy. The Data Retention Policy specifies retention periods for different categories of data based on legal, regulatory, and business requirements, and outlines secure disposal methods.

6. ARTIFICIAL INTELLIGENCE:

This pillar set outs the criteria for how Artificial Intelligence (AI) may be used by the Trustees in running the Scheme for the benefits of the members.

Supporting Policy:

(a) Artificial Intelligence Policy: This policy specifies the cases for the use of AI when working on the Scheme. This covers the principles of transparency, accountability, data protection, security and confidentiality; and compliance and ethics. It also covers permitted and prohibited uses and roles and responsibilities.

7. Information Security:

Information security is critical for protecting the Scheme's data assets from various threats, ensuring their confidentiality, integrity, and availability. This pillar encompasses the implementation of robust technical and organisational controls to safeguard data and systems.

Supporting Policy:

(a) Information Security Policy: This policy establishes the framework for protecting the Scheme's information assets, covering areas such as risk management, access control, network security, endpoint security, data encryption, and security monitoring.

8. ICT Risk Management Framework:

This pillar focuses on enabling the Trustees to address Information and Communications Technology (ICT) risks quickly, efficiently and comprehensively and to ensure a high level of digital operational resilience. The Trustees focus on managing the risks associated with third-party service providers who process Scheme data or provide critical ICT services. It ensures that appropriate due diligence, contractual agreements, and ongoing monitoring are in place to protect the Scheme's data and operational resilience. This pillar addresses the Scheme's ability to withstand, respond to, and recover from ICT-related disruptions, as mandated by the Digital Operational Resilience Act (DORA).

Supporting Policies:

(a) Outsourcing Policy: This policy establishes the framework for outsourcing service providers and advisors, contract terms, process for selection and appointment of third-party service providers.

(b) Business Continuity Plan: This documents how the Trustees will organise themselves when there is a disruption to the activities of the Trustee Board.

(c) Operational Resilience Policy: This policy details the framework for identifying, assessing, and managing ICT risks, including incident classification, setting recovery time objectives and recovery point objectives, disaster recovery, and incident management specific to ICT including reporting to Regulators and others.

(d) Register of Information: This contains details of ICT third-party providers.

9. COMPLIANCE AND REPORTING:

This pillar ensures continuous monitoring of compliance with all relevant data governance requirements and facilitates timely and accurate reporting to regulatory bodies and internal stakeholders. The Trustees receive periodic assurance, via reporting or review, that the policies and procedures are being operated effectively.

Supporting Procedure:

(a) Governance & Compliance Calendar: The Calendar is used to monitor adherence to data governance policies, conducting internal audits, and preparing reports for the Trustee Board and regulatory authorities.

10. LEGAL STANDING:

This Data Governance Framework, and the supporting policies and procedures, is a high-level non-binding document prepared for the purposes of the Scheme's governance. It is not, nor is it intended to be, a legal document and is not intended to have legal effect or to be legally binding on the Trustee Board, nor to override the Trust Deed & Rules of the Scheme.

The Trustees reserve the right at all times to depart from the terms of this Framework as it sees fit; for example, to accommodate a particular set of circumstances or a changing of views. Any departure will be exceptional, documented and approved by the Trustees.

11. REVIEW:

This Data Governance Framework, and the supporting policies and procedures, must be reviewed at least once every three years, or sooner, if the Trustee Board are of the view that circumstances warrant it. Some supporting policies may be reviewed more frequently to reflect operational (e.g. pace of change – AI Policy) or regulatory requirements (e.g. Data Strategy Policy). The Trustees will maintain documented evidence of their review.

12. CONCLUSION:

This Data Governance Framework provides a robust and adaptable structure for the National Federation's Pension and Life Assurance Scheme to manage its data assets effectively, protect member information, enhance operational resilience, and maintain regulatory compliance. The detailed implementation of this framework is achieved through the comprehensive suite of supporting policies and procedures, which will be regularly reviewed and updated to adapt to evolving threats and regulatory landscapes.

REFERENCES:

(a) The European Union (Occupational Pension Schemes) Regulations 2021, S.I. 128/2021 (implementing the terms of Directive (EU) 2016/2341 of the European Parliament and of the Council of 14 December 2016) on the activities and supervision of institutions for occupational retirement provision (IORPs)

(b) Pensions Authority Code of Practice for trustees of occupational pension schemes and trust retirement annuity contracts (November 2021)

(c) General Data Protection Regulation (EU) 2016/679

(d) Irish Data Protection Act 2018

(e) Digital Operational Resilience Act (EU) 2022/2554 (DORA)

End

Approval and Next Review Date of this Policy:

This document was approved and came into effect as follows:

Document Control	
Approved By:	Mr. James Skehan Chairman & Professional Trustee, National Federation of Voluntary Service Providers' Pension & Life Assurance Scheme
Approved By:	Mr. John McHugo Vice Chairman, National Federation of Voluntary Service Providers' Pension & Life Assurance Scheme
Date approved:	30th July, 2026
Next review date	30th July, 2029
Previous versions	30th October 2025

Signed: ______________________________ **Date: 30th July, 2026**

James Skehan,
Chairman & Professional Trustee.

Signed: ______________________________ **Date: 30th July, 2026**

John McHugo,
Vice Chairman.

a Oranmore Business Park, Oranmore, Galway, Ireland, H91 TP2W.
t + 353 (0)91 792316 e pensionadmin@fedvol.ie w www.fedvol.ie
Pension Authority No: PB67866 Revenue Approval No: SF7346

Appendix 1 – Policy Cross Reference Guide

Further to the Data Governance pillars shown in section 1 above, this diagram shows the main policies under each pillar and supporting policies and procedures.