Informal Commission Expert Group on the Next Generation European Interoperability Framework (EIF) recommendations for

Next Generation EIF Blueprint

<mark>Draft 0.2</mark>

<mark>15th November 2025</mark>

Disclaimer

This document represents the proposal of the Informal Expert Group on the Next Generation European Interoperability Framework (hereinafter referred to as Expert group) for a blueprint of the Next Generation European Interoperability Framework. It aims to propose the structure and contents of the framework.

This document has been prepared by the Informal Expert Group on the Next Generation European Interoperability Framework (hereinafter referred to as Expert group) in accordance with individual expert agreements (hereinafter referred to as Agreements), considering requirements defined in the Expert call for expression of the interest.

The document contains information obtained from various sources (EU stakeholders' survey, experts' survey etc.). The Expert Group has not attempted to verify the reliability of the sources or the information provided. Therefore, the Expert Group does not make any representations or warranties (express or implied) to any person other than European Commission under the Agreements regarding the accuracy or completeness of the document.

This is a draft document. The comments expressed in this draft document are subject to change or withdrawal, only those expressed in the final text of the deliverable will be considered conclusive.

We draw your attention to the relevant comments in the document regarding the scope of work, the purpose of the deliverable, assumptions, and the limitations on the information on which our deliverable is based (Section 1).

Any questions regarding this document should be addressed to the Secretariat of the Interoperable Europe Board at EC-INTEROPERABLE-EUROPE-BOARD@ec.europa.eu

Table of Contents

1.Introduction

1.1 Why is interoperability important?

Interoperability is the cornerstone of effective, citizen-centric digital public services, as it enables public administrations, businesses, and individuals to exchange data and operate seamlessly across organisational, sectoral, and national boundaries. Without interoperability, the digital transformation of government remains fragmented. The goal is to avoid each system locked in its own silos, unable to share information or coordinate decisions efficiently.

By contrast, when data, processes, and services are interoperable, administrations can deliver faster, more transparent, and user-friendly services, reduce administrative burdens, and ensure that citizens and businesses interact with government only once for each need. Interoperability thus creates tangible public value: it enhances trust, supports evidence-based policymaking, facilitates cross-border cooperation, and drives innovation through the reuse of digital solutions.

Ultimately, it turns Europe's diversity of systems and institutions into a coherent and connected digital ecosystem, reinforcing both single market and democratic governance in the digital age.

1.2 Why do we need the EIF?

The **European Interoperability Framework (EIF)** arises from the need to provide a common legal, organisational, semantic and technical foundation for the seamless exchange of data and services across public administrations in Europe. In an environment where governments, businesses and citizens increasingly rely on cross-border digital interaction, the absence of shared standards and specifications, reference architectures and coordination mechanisms can lead to fragmentation, inefficiency and duplication of effort.

The **Interoperable Europe Act** (IEA) directly addresses this challenge by establishing interoperability as a legal obligation and by mandating the creation of shared solutions for public administrations. Within this framework, the EIF becomes the conceptual and operational reference that guides Member States and EU institutions in developing digital public services that can interact natively, safely and meaningfully.

The EIF provides a set of principles and recommendations to enhance interoperability in the EU. For its practical implementation, it relies on tools and instruments in the IEA. Central among these are the interoperability solutions: reusable assets addressing legal,

organisational, semantic, or technical requirements that enable cross-border interoperability. They operationalise the EIF and provide stakeholders with concrete means to design and manage interoperable public services, such as the European Interoperability Reference Architecture. To further guide implementation, a subset of these solutions, labelled as Interoperable Europe Solutions, will be gradually endorsed by the Interoperable Europe Board. These provide additional guidance to stakeholders by highlighting relevant solutions, supporting consistent and effective implementation of the EIF across the EU.

This revision therefore responds both to an institutional demand - ensuring that EU policies are implemented coherently across Member States - and to an operational need, providing the framework, shared vocabulary and governance model that enables truly interoperable public services throughout the European Union.

1.3 What is the scope and objective of the EIF?

The EIF defines common principles, reference models and recommendations that together guide the regulation, design and delivery of digital public services working across organisational, sectoral and national boundaries. The EIF serves as the umbrella reference for the European public sector's digital transformation, ensuring that efforts of administration and businesses converge toward a common European digital space.

It is called **European** because it represents a collective commitment, an agreement among Member States and EU institutions, to achieve interoperability as a shared public value and a practical enabler of the Single Market. The term **Interoperability** signals its legal foundation in the regulation and emphasises a focus on practical operability between organisations collaborating on integrated service delivery. By naming it a **Framework** it signals a distinction from binding legal requirements, standards or architectures to be implemented directly, but rather a set of long-lasting principles and high-level conceptual models to guide more collaboration at all levels of government towards to shared goal of coherent, efficient and trusted digital public services in Europe.

An explicit objective of the EIF is to support the instruments in the IEA. The EIF is to be used directly in the **Interoperability Assessment Mechanism.** The reference models and principles will serve as a starting point for local practices and support a common structure when comparing assessments across solutions and across levels of government. EIF has a cascading effect into **National Interoperability Frameworks (NIFs)** and **Specialised Interoperability Frameworks (SIFs)**. The EIF provides a common foundation and can help drive convergence, identify conflicting interests and easy comparison through shared reference models. Ideally the individual elements of the EIF are strategic building blocks that

can be adopted directly or adjusted to fit more specific context. The EIF shall guide the criteria used by the Interoperability Board when labelling **Interoperable Europe Solutions** and support organise of the **Catalogue** for reusability and monitoring purposes.

The **EIF** is not a technical architecture. Unlike the **European Interoperability Reference Architecture (EIRA)**, which provides detailed architectural views and reusable solution components, the EIF does not prescribe specific system designs or technological blueprints. Equally, it differs from the **IEA**, which establishes the legal and institutional basis for cooperation, obligations, and governance in interoperability across the European Union.
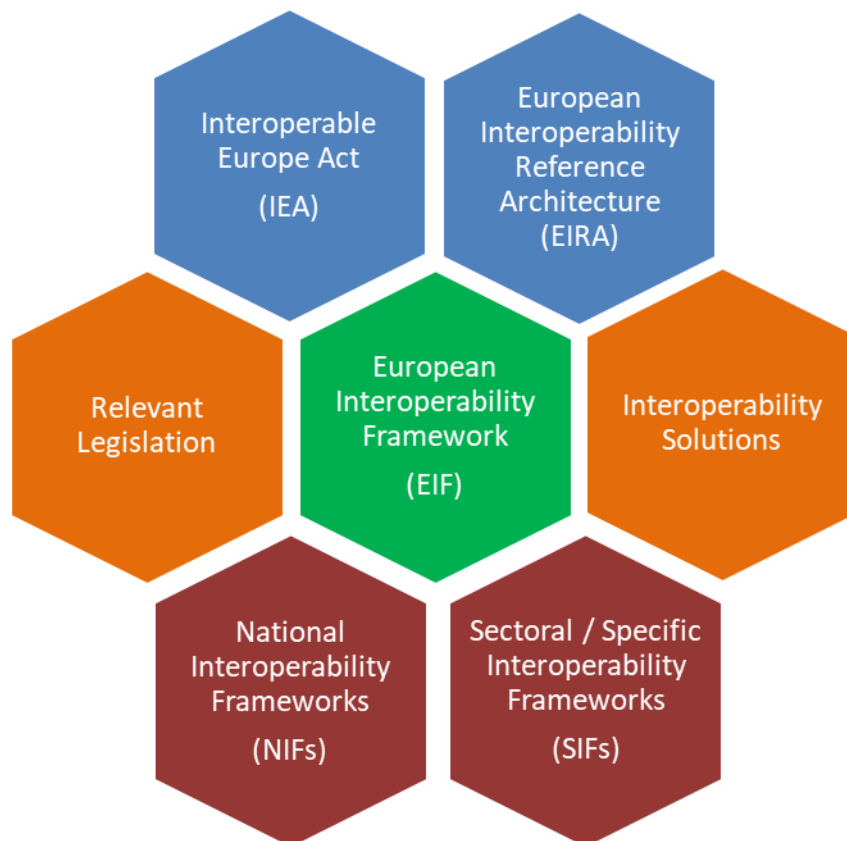
Figure 1: The Context of the EIF

1.4 Revision of the framework

The revision of the EIF responds to new policy and technology realities and must be anchored in the Interoperable Europe Act, while remaining compatible with the broader EU policy. The update process takes into account how the current EIF integrates legal and policy frameworks and ensures that new developments are considered in the next version

of the EIF. In addition, the Interoperable Europe Act and EIF share a special relationship, reinforcing each other and together setting the overall governance of interoperability in the EU.

A special relationship: the Interoperable Europe Act:
- The EIF supports the implementation of the Act, as it has to be considered when conducting legal interoperability assessments, in line with Art. 6.2. In addition, the Act itself supports the further uptake of the EIF and provides a governance structure that fulfils roles of further development, monitoring, and oversight.
- In accordance with the Act, the new EIF should continue to promote multilingualism in the public sector, openness (open source, open standards, open data), accessibility, technical neutrality, reusability, security and privacy (Preamble §29, §35).

Funding programme:
- Currently, the **Digital Europe Programme** is supporting improvements in interoperability through EU funding for interoperability actions (Specific Objective 5 of the Programme). Synergies in terms of funding are essential to ensure interoperability goals can be practically implemented and financially supported.

Regulatory frameworks already referenced in the EIF or for which the EIF evaluation indicated a certain level of alignment:
- **eIDAS Regulation**, providing the trust-service and electronic-identity backbone for cross-border digital public services
- **INSPIRE Directive**, domain-specific example of an interoperability framework integrating EIF guidance (establishing an infrastructure for spatial information)
- **Open Data Directive**, promoting the sharing, use and reuse of public sector data
- **Single Digital Gateway**, building on EIF guidance to provide users with a single point of access to digital services, information and, administrative procedures on a cross-border basis

New regulatory frameworks for the digital economy and emerging technologies currently not taken into account in the EIF:
- **Data Governance Act –** establishes the European Data Innovation Board and common governance rules for data-sharing services, which the EIF should reference in order to adequately address developments related to data-driven services and the EU Data Spaces

- **Artificial Intelligence Act** – introduces requirements for AI transparency and interoperability; the EIF should consider embedding AI-specific interoperability guidelines.
- **EU Digital Identity Wallet** – upcoming trust-service and digital-identity framework that will become the de-facto cross-border identity layer for public services.
- **EU Data Spaces** (e.g. mobility, health, energy etc.) – the new EIF should consider developments related to data spaces as use cases for the need for enhanced interoperability. Sector specific guidance, on top of the EIF will be necessary to fully develop the data spaces, but the EIF should remain as the common, minimum standards basis.

Lessons from practice underline that the 2017 version of the EIF can be too generic and that capability-driven, actionable guidance with showcases is needed. The evaluation of the EIF published in 2021 provided a basis for the review process, outlining several key aspects that the next EIF should consider. The evaluation highlights the need to make the framework more practical, actionable, and widely adopted. While its strategic vision is valued, practitioners require clearer guidance, linked solutions, and shared best practices to support implementation. Awareness remains limited, especially at local levels, and sustainability depends on adequate resources, planning, and cultural change. Stronger coordination and potentially more binding rules may be needed, based on the results of the evaluation, to ensure consistent cross-border interoperability, while monitoring should focus on reuse and costs. Aligning the EIF with emerging digital policies is key to its continued relevance and impact.

Against this background, the Commission's Directorate-General for Digital Services ('DG DIGIT') decided to set up an informal expert group on the Next Generation EIF to support the implementation of the Interoperable Europe Act. More specifically, the group on the Next Generation EIF has been tasked to provide independent expert advice on the scope, priorities and added value of the Next Generation EIF. By providing a blueprint for the Next Generation EIF, the group will allow policy makers to feed into discussions on the revision and highlight problems that would require systematic address.

The process of updating the EIF was led by lessons learned and new policy priorities, ensuring it stays relevant and actionable in today's digital landscape:

- **Build on the 2017 EIF:** The update process built on the current EIF and take into account feedback collected through the evaluation of the EIF, the monitoring of the

implementation of the EIF, as well as additional stakeholder feedback collected as part of the work of the Informal Expert Group[1].

- **Respond to change:** It addresses technological advances (e.g. on AI, IoT interoperability, blockchain), political shifts and evolving strategic priorities such as digital sovereignty.
- **Foster synergies:** The revision showcases the close interlinkages between the EIF and existing and emerging EU legal and policy frameworks, from the Interoperable Europe Act and eIDAS to the Data Governance Act, Common Data Spaces, and AI Act.

1.5 Structure and key terms

This document is organised into five main chapters, each addressing a specific part of the framework's logic.

Chapter 1 introduces the background, objectives and definitions forming the conceptual foundation of the EIF.

Chapter 2 describes the stakeholder ecosystem and application scenarios in which the EIF operates, identifying the key stakeholder groups, the roles of the main actors in digital public service provision that would be a typical audience of the EIF and the main application scenarios for the EIF.

Chapter 3 presents the principles, the core set of normative guidelines that express the values, priorities and practices for achieving interoperability in digital public services.

Chapter 4 translates the principles into recommendations, offering actionable guidance for specific application scenarios such as policy formulation, service design, ICT components creation and legislative drafting.

Chapter 5 provides further guidance, detailing how to apply the EIF in practice through the development of National Interoperability Frameworks, the use of Interoperable Europe Solutions, training, testing, and other governance mechanisms.

Complementary annexes and online catalogues list the relevant legislation, reusable artefacts, and EU infrastructures (e.g. EIRA, SEMIC, OOTS, eTranslation, Data Spaces) that provide the operational context of the EIF. This structure aims at making the EIF function

---

[1] Through a public consultation on the Interoperable Europe Portal.

both as a strategic reference for policymakers and as a practical guide for implementers of interoperable digital public services.

The following table presents the definitions of the key terms used throughout the EIF, serving as a reference point for policymakers, architects, and implementers of digital government solutions.

Table 1: Key terms of the EIF and their definitions

(EIF) Stakeholders	EIF stakeholders are the public, private, and societal actors who influence, apply, or benefit from interoperability in the European public sector. Together, they form the ecosystem that designs, governs, implements, and uses interoperable digital public services across Europe.
(EIF) Stakeholder Roles	EIF stakeholder roles describe the distinct functions and responsibilities each stakeholder or specific actor assumes in achieving interoperability. Understanding these roles helps coordinate efforts and ensure shared accountability within the interoperability landscape.
(EIF) Application Scenarios	EIF application scenarios illustrate how interoperability principles and recommendations can be applied in practice across the public-sector lifecycle. Each scenario demonstrates how coordinated use of legal, organisational, semantic, and technical interoperability can improve coherence, efficiency, and trust in European digital public services.
(EIF) Principle	An EIF principle is a foundational guideline that expresses a core value or best practice to be followed when designing, implementing, and governing interoperable digital public services in Europe. Each principle of the EIF captures a key aspect of how administrations should collaborate, manage data, use technology, or serve citizens and businesses across borders. Together, the EIF principles form the normative backbone of the European Interoperability Framework.
(EIF) Recommendation	An EIF recommendation is a concrete, actionable instruction derived from the EIF principles, providing specific guidance on how public administrations should achieve interoperability in practice. While principles express the "why" and "what" of

	interoperability, recommendations define the "how" — outlining steps, methods, or standards to be adopted at legal, organisational, semantic, or technical level.
(EIF) Interoperability Layer	An interoperability layer is a specific view, aspect or dimension of the overall interoperability framework that describes how public administrations, organisations, and systems cooperate and exchange information effectively. Each layer addresses a different perspective: legal, organisational, semantic or technical interoperability, as well as the cross-cutting interoperability governance.
Interoperability Solution	An Interoperability Solution is a reusable asset concerning legal, organisational, semantic or technical requirements to enable cross-border interoperability, such as conceptual frameworks, guidelines, reference architectures, technical specifications, standards, services and applications, as well as documented technical components, such as source code.
Interoperable Europe portal	The portal which serves as a single point of entry and provision, for information related to cross-border interoperability of trans-European digital public services.
Interoperable Europe solution	A recommended Interoperability Solution for the cross-border interoperability of trans-European digital public services, carrying the relevant label given by the Interoperability Board and published on the Interoperable Europe portal.

2. Stakeholder Ecosystem and Application Scenarios

2.1 Stakeholder Groups

The ecosystem of organisations involved in European cross-border digital public services is extensive, multi-layered, and increasingly influenced by global developments. This section provides a typology of stakeholder groups that are central to the EIF. Defining this typology is an essential step toward recognising the varied interoperability needs across the public sector, identifying how different actors interact and affect one another. Furthermore, it ensures that the EIF responds effectively to these dynamics.

At the highest level, the principal stakeholders of the EIF can be grouped into three broad categories: A (administrations), B (businesses) and C (citizens). Recognising these three groups ensures continuity with the 2017 EIF and the ISA[2] programme, both of which explicitly identified them as the main beneficiaries of interoperable public services. This framing is also consistent with international practice, as reflected in the work of the OECD, the World Bank, and the United Nations on digital public infrastructure, public services, and interoperability. These organisations highlight how interoperable systems strengthen administrative efficiency and enhance accessibility and service quality for citizens and businesses.[2] The three categories can be described as follows:

A- **Administrations** include all public sector bodies, governments on European, national, regional and local levels, public organisations, and public sector-owned service organisations.

B- **Businesses** include privately controlled companies (large, small and medium sized, or very small) with activities on international, European, national and/or local level, and their supporting associations.

C- **Citizens** are physical persons residing in EU Member States, their supporting associations, NGOs and the civic society in general. The term also includes all individuals in general with fundamental rights.

---

[2] OECD. 2024. *Digital Public Infrastructure for Digital Governments*; World Bank.2022. *Interoperability: Towards a Data-Driven Public Sector*; UN, Universal DPI Safeguards Framework. The UN DPI framework refers to individuals, civic and public authorities, and private entities.

2.2 Stakeholder roles

The effective implementation of the EIF relies not only on identifying who the stakeholder groups are, but also on understanding **the distinct roles** each actor may play within the interoperability ecosystem. Each role contributes to shaping, operating, or sustaining interoperable digital public services.

Clarifying these roles helps define **responsibilities, dependencies, and collaboration pathways** across governance levels. It also ensures that interoperability is addressed consistently throughout the policy, design, and delivery of digital public services.

By mapping these roles, the EIF provides an operational perspective on *where* coordination, capacity building, and common specifications are most needed to achieve a connected and effective European digital administration.

Public Service Consumers

Every citizen, business and even administrations are consumers of digital public services. Service consumers are the direct and most important beneficiaries of a higher degree of interoperability. From an inner-market perspective, users that are consuming services across borders are of special interest. Service consumers benefit from interoperable services, by reduced perceived complexity, effective use of devices and data across services, and indirectly through lower cost of providing public services.

Legislators

Legislators create binding legal requirements through parliamentary or equivalent processes. They define laws that shape the operation of public services, whether targeting specific services, sectors, digital technology use, or the general functioning of public administrations, based on societal needs. Their role is primarily normative and formal, providing the rules governing public services.

Policymakers

Policymakers set strategic directions and priorities that guide how organisations operate within the legal framework. They operationalise rules and drive the development and improvement of public services, coordinating initiatives both within individual organisations and across the broader system. Policymakers also identify gaps or emerging needs that can inform the evolution of legislation over time. Unlike legislators, they do not create binding laws but contribute to how rules are applied, interpreted, and adapted. Citizens, including civil society, influence policy through advocacy or political engagement, helping to inform and steer these strategic decisions.

Service Designers

Public and private services are the results of deliberate design processes. Often with a strong focus on ease of use, efficiency and overall value proposition for both providers, consumers and society in general. Designers form different communities of practices across administrations, business and citizens, provide formal education and establish research disciplines. A service design results in requirements for its various users and most comply with a growing number of horizontal regulations both within a sector and across them. Service designers benefit from interoperability through reuse of existing solutions for common problems (patterns).

Public Service Providers

Administrations on every level provide some form of public service. With the growing degree of digitalisation of society in general, most, if not all, services will involve some kind of direct or indirect digital interaction. Providers of public services rely on private services to operate, and private services often rely on some public services or are required by law to interact directly with public services. Service providers benefit from interoperability when building service with a high degree of reuse of existing services, data and products and cheaper private digital products through market mechanisms.

Data Providers

Digital public services consume data which is processed (especially registered, stored and exchanged) in a variety of contexts within these services. Administrations maintain base registries, statistics, records of individual decisions and historical data – business records of product properties, transactions from providing services and other customer interactions – citizens record of their transactions with services and private records of everyday life events.

ICT Providers

Digital Public services are implemented using technology provided by an ecosystem of products and services from the private sector. Service consumers access digital public services through products and custom-built ICT systems. Administrations procure products and services implementing technical specifications and harmonised standards. ICT providers work together to establish and maintain technical interoperability between products.

Standardisation bodies

Businesses collaborate on technical specifications and other standards through a network of standardisation organisations that align and resolve contradicting requirements. Administrations can use existing standards to support effective procurement and formally request new standards to be developed. Citizens can influence Businesses to include special interests in standardisation through collaboration in the development process. Standardisation organisations benefit from interoperability frameworks to help identify product and service categories and form alignment and clarification of legal requirements in markets.

The following table depicts the mapping of EIF stakeholder roles, linked to stakeholder categories, their expected contributions to interoperability and the main interoperability benefits.

Table 2: Stakeholders, their contributions and benefits

Stakeholder role	Contributions	Benefits
Public Service Consumers (ABC)	Feedback on existing services Demand for new and better services Influence through civic organisations	Access (easier) to cross-border services Better user experience Stronger security, privacy and trustfulness More control over data (re)-use Indirect savings through efficiency
Public Service Providers (A)	Authority of data and public data Regulatory enforcement Investments in ICT solutions and digital infrastructure Investments in standardisation	Reuse of existing data and solutions Lower ICT cost through market mechanisms Efficient service delivery Support for ICT procurement
Service Designers (ABC)	Expertise in user experience Design methodologies Service innovation	Access to interoperability solutions Efficient assessments through alignment Faster design cycles and improved service quality
Legislators (A)	Translating strategy and policy into law Consistency of legislation High-level legal frameworks	Improved regulatory coherence Feedback from implementation of law
Data Providers (ABC)	Support of data communities Technical support for data reuse	Broader use and recognition of their datasets Value generated from data reuse and linkage Overview of existing solutions for reuse

Stakeholder role	Contributions	Benefits
Policymakers (AB)	Strategic direction Reporting on uptake Collaboration agreements	Access to interoperability solutions Policies and measures that promote sustainable digital transformation of the public sector
Standardisation Bodies (B)	Technical specifications and standards Established collaborations Shared interest in interoperability	Standardisation request and funding European footprint in global standardisation More usage of standards and services
ICT Providers (B)	Existing and new solutions Existing technical interoperability Competition on quality and cost	Market alignment of industry and public-sector Common requirements from customers

2.3 Application Scenarios

The EIF operates across a wide range of application scenarios that reflect the key processes through which public administrations design, implement, and evolve digital public services. These scenarios illustrate how interoperability principles and recommendations can be applied in practice; from the earliest stages of drafting legislation and formulating policies, to the operational realities of designing and delivering services, and the technical dimension of developing interoperability solutions.

The scenarios below provide concrete guidance on how to embed interoperability "by design" into public sector activities, ensuring consistency, reusability, and efficiency across all layers of digital governance in Europe. Each scenario represents a critical point in the policymaking and service delivery cycle where collaboration, data sharing, and alignment of systems are essential.

Application Scenario 1: Drafting legislation

Interoperability begins at the legislative level, where laws and regulations define the framework within which digital public services operate. Applying the EIF to the drafting of legislation ensures that legal instruments are consistent, machine-readable, and designed to enable rather than constrain data sharing and cross-border collaboration. This involves aligning terminology, referencing common data models, and embedding provisions that facilitate the recognition and exchange of electronic documents, identities, and administrative acts across Member States. An early consideration of interoperability dimensions in the law-making process enables administrations to prevent legal fragmentation and creates a foundation for coherent digital governance.

Application Scenario 2: Formulating Policies

Policy formulation relies increasingly on the collection, analysis, and integration of data from multiple sources and jurisdictions. Applying the EIF to policy design and decision-making allows policymakers to base their strategies on interoperable information flows, shared indicators, and common standards. It enables Digital-Ready Policymaking and interoperability assessments, ensuring that policies, data platforms, and digital solutions are designed for reuse and compliance with existing legislative frameworks. It promotes data-driven collaboration beyond mere data collection, supporting coherent, future-proof, and interoperable policymaking across the EU. Overall, this application scenario enables more evidence-based and coordinated policymaking, ensuring that policy objectives are aligned across sectors and countries. The application of interoperability in policy design supports the coherence between EU and national priorities, fosters transparency, and facilitates the monitoring and evaluation of outcomes.

Application Scenario 3: Designing and delivering services

Interoperability is most visible in the design and delivery of public services, where citizens and businesses interact directly with administrations. Applying EIF principles and recommendations in this application scenario ensures that services are user-centric, accessible, and seamlessly connected across institutions and borders. This includes aligning business processes, integrating shared data infrastructures, and reusing digital components to reduce administrative burden. Governments, departments and projects embed interoperability into service design, effectively moving from fragmented solutions to coordinated service ecosystems that deliver consistent and efficient experiences for users throughout Europe.

Application Scenario 4: Developing interoperability solutions

The EIF also guides the development of interoperability solutions — reusable assets such as standards, alignments, reference architectures, data models, software components, and APIs that enable systems to communicate and operate together. These solutions translate policy and legal requirements into technical artefacts that can be widely adopted across Member States and levels of government. The focus on promoting openness, modularity, and reuse ensures that investments in interoperability generate long-term value and reduce duplication. Developing such solutions within the Interoperable Europe framework strengthens cross-border cooperation, accelerates innovation, and supports the creation of a truly interconnected European digital ecosystem.

Achieving Interoperability in Digital Governance

Developing Solutions
Building reusable assets for system communication

Designing Services
Creating user-centric and seamlessly connected services

Formulating Policies
Basing strategies on interoperable information flow

Drafting Legislation
Ensuring legal instruments are consistent and enable data sharing
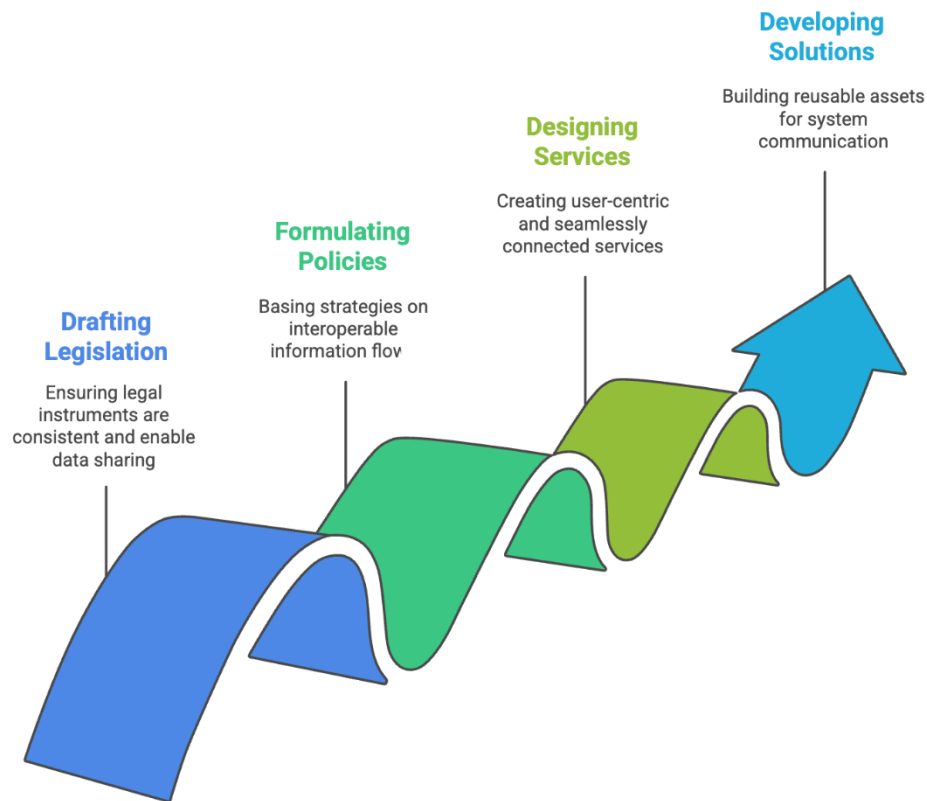
Figure 2: Application scenarios

2.4 Interoperability Layers

The EIF is structured around four distinct but interrelated layers of interoperability and a cross-cutting concern that together ensure coherent collaboration among public administrations and businesses. These layers provide a comprehensive perspective, addressing all dimensions required for systems, organizations, and policies to work together effectively. By considering interoperability through these layered viewpoints, the EIF offers a holistic model that connects legal and institutional alignment with semantic consistency, technical integration, and coordinated governance, enabling digital public services to function seamlessly across borders and sectors.

Legal Interoperability

The layer of interoperability which ensures that organisations working together under different legal frameworks can interoperate by addressing laws, regulations, policies and other binding requirements that enable or constrain data and service exchange.

Organisational Interoperability

The layer of interoperability which focuses on aligning business processes, roles and responsibilities of organisations providing or using public services, and typically includes collaboration agreements, process choreographies, and other elements of governance.

Semantic Interoperability

This layer ensures that the meaning of exchanged information is preserved and understood by all collaborating parties and systems, dealing with data models, vocabularies, ontologies, code lists, and various forms of metadata.

Technical Interoperability

The layer of interoperability which covers the technical enablers for connecting systems and services, such as technical infrastructures and ICT components that enable communication and data exchange.

Interoperability Governance

This layer refers to the set of structures, processes, and mechanisms that ensure coordinated management, oversight, and evolution of interoperability across public administrations in Europe. It encompasses the policies, roles, responsibilities, and decision-making arrangements that guide how interoperability frameworks, specifications, requirements or standards are developed, maintained, and adopted.

2.5 Connecting the EIF Elements

To provide a coherent structure but also cater for multiple views towards different stakeholders and needs, all the elements of the EIF are connected together at the recommendations level. Following this approach, each EIF recommendation:

- belongs to an application scenario
- concerns one or more stakeholder roles
- is derived from one or more principles
- is categorised along the respective interoperability layers
- might reference relevant legislation or interoperability solutions, external to the EIF
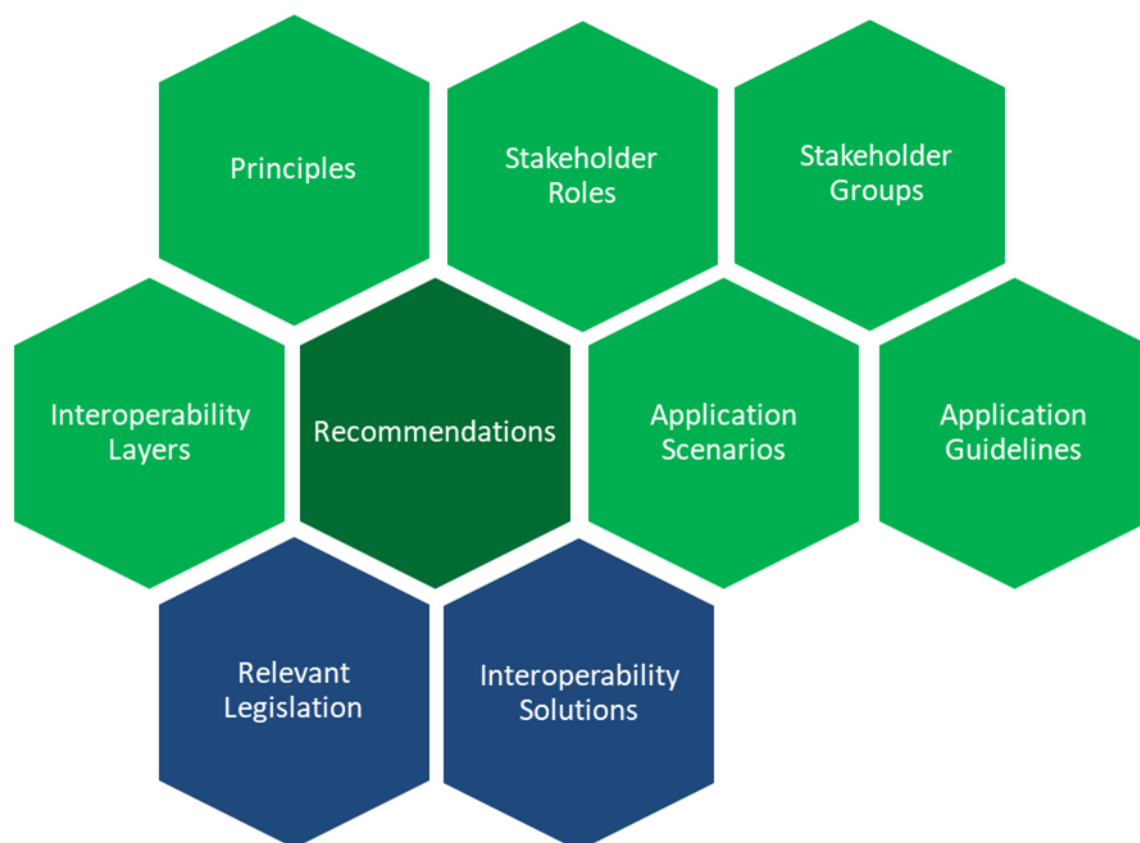
Figure 3: Contents of the EIF (in green) and referenced external elements (in blue)

3. Principles

The EIF is built on top of a set of principles that represent the core values of the framework. They must be considered in full to ensure consistent, high-quality interoperability outcomes in the context of public services. They can be implemented across multiple governance levels such as the local, regional, national, and European level. Principles are complementary to existing legislation, ensuring alignment with EU law while promoting practical coherence in its application.

Each principle is presented with a rationale (why it matters), a description (what it entails), and a potential implication (how it improves interoperability). Together, they guide the application of the EIF across its five interoperability layers and four application scenarios, forming the foundation for an interconnected and trusted European digital ecosystem.

Update of the principles

The principles included in the 2017 version of the EIF have been updated to include recent developments. For example, the overemphasis of "openness" has been removed: this indeed is important for open data, which is handled by its respective directive. Openness and open data are now targeted by other principles indirectly. Technological Neutrality & Data Portability, Inclusion & Accessibility, and Multilingualism also were reframed in new principles.

Principle 1: Subsidiarity and proportionality

"Right level, right action: subsidiarity and proportionality in interoperability"

Rationale. Subsidiarity and proportionality ensure that decisions and actions are taken at the most effective level, while avoiding unnecessary burdens. The subsidiarity principle requires that decisions are made as closely as possible to the citizen, while the proportionality principle, as established in the EU founding Treaties, limits EU actions to what is strictly necessary to achieve their objectives. This ensures that EU-level interventions only occur when they add clear value and cannot be achieved as effectively by Member States alone, supporting trust and legitimacy in digital public services.

Description. The principle of subsidiarity requires that interoperability-related decisions and actions are taken at the appropriate level of governance - local, regional, national, or EU - where they are most effective and relevant. Proportionality ensures that any measures adopted are strictly necessary to achieve interoperability objectives, without imposing

undue constraints or costs. In the EIF, this means aligning national and EU frameworks, harmonising standards where beneficial, while still allowing for tailored solutions that address specific needs. The principle guides the design and implementation of interoperability solutions, ensuring they are context-sensitive, efficient, and respectful of Member States' autonomy while fostering cross-border collaboration.

Implications. Applying subsidiarity and proportionality means that interoperability solutions must be designed to accommodate both harmonised standards and local specificities. Administrations at all levels are responsible for ensuring that digital public services are accessible, relevant, and trusted by citizens, while also supporting cross-border data exchange and collaboration. In line with the Treaties, this principle limits EU actions to what is necessary for interoperability, reducing regulatory fragmentation and encouraging innovation by allowing flexibility in implementation. It requires balancing standardisation with adaptability.

Principle 2: Transparent by design

"You can't trust what you can't understand."

Rationale. Transparency is a fundamental principle for building trust, accountability, and legitimacy in digital public administration. As governments increasingly rely on data-driven systems, interoperability frameworks, and artificial intelligence, it becomes essential that administrative processes, decisions, and digital services remain open and understandable to citizens and stakeholders. Transparency enables informed participation, oversight, and collaboration within and across public sector entities, while safeguarding ethical and lawful data use. It also underpins algorithmic accountability by ensuring that automated and AI-supported decisions can be explained, audited, and aligned with democratic principles, human rights, and the rule of law.

Description. Transparency refers to ensuring visibility and traceability across the administrative ecosystem, allowing administrations, businesses and citizens, , to understand rules, processes, data, and decision-making, including those supported by artificial intelligence and automated systems. It requires that public sector information systems provide interoperable and well-documented interfaces, guaranteeing secure and lawful access to data while upholding the principles of data protection and privacy. Transparency also encompasses explainable and accountable AI, ensuring that algorithmic decisions remain understandable, auditable, and under meaningful human oversight. An ethics-by-design approach, which integrates ethical principles and human values

throughout the entire AI lifecycle, works alongside transparency to foster trust, inclusiveness, and integrity in digital public services.

Implications. Transparency enhances trust and accountability in public sector interoperability by making data use, decision-making, and automated processes understandable and verifiable. It strengthens compliance with legal and ethical standards, reinforces citizens' rights, and supports the responsible and trustworthy use of emerging technologies in government. Transparency in data provenance, ownership, and governance facilitates interoperability and cross-border collaboration, enabling evidence-based policymaking and ensuring digital public services across the EU remain open, fair, and aligned with democratic values.

Principle 3: Efficiency through reuse

"Build once, reuse many times."

Rationale. Reusability is the cornerstone of efficient public service delivery. It directly reduces costs and time to implement new solutions, limits fragmentation of the IT landscape, and guarantees high service quality. The principle mandates that interfaces, standards, information, and digital building blocks are designed for multiple operational uses across all sectors and administrative levels. This approach allows administrations to redirect resources from basic infrastructure development toward value-added innovation, thus enabling true cross-level, cross-sector, and cross-border collaboration.

Description. Reusability in the EIF context means actively designing, procuring, and utilising solutions so they can be adopted multiple times across various contexts and jurisdictions, fostering a shared ecosystem of assets. This encompasses a broad range of activities aimed at ensuring interoperability, reuse, and trust across digital systems. It involves the standardisation and profiling of solutions through established specifications, such as DCAT-AP and INSPIRE for data and geoinformation, HL7 FHIR for healthcare, and ISO 20022 or PSD2 for financial services; to guarantee semantic and technical compatibility. Cataloguing and discovery mechanisms enable the registration of reusable artefacts, including data models, Core Vocabularies, API patterns (OpenAPI), and integration libraries, within organisational, national, and EU-level repositories to promote visibility and reuse. A clear framework for licensing and metadata supports legal certainty and transparency by defining permissive licences (e.g. EUPL, MIT) and including detailed metadata on versioning, ownership, and conformity status. The Components as Services approach furthers modularity and scalability by exposing complex functionalities as versioned, contracted microservices with defined Service Level Objectives (SLOs/SLIs) and prebuilt adapters for

integration with domain systems. Moreover, data and AI assets are managed as reusable products, governed by defined schemas, quality and access agreements, and supported by Machine Learning Operations (MLOps) practices and model cards for AI/ML components. Robust governance and compliance mechanisms, covering review, certification, and maintenance, ensure that all reusable building blocks remain aligned with key European frameworks such as eIDAS, eDelivery, GDPR, and NIS2.

Implications. The adoption of proven, standardized components drives significant operational efficiency, leading to faster project delivery, easier systems integration, reduced defects, and simplified maintenance. This foundation of efficiency directly contributes to economic sustainability by lowering the Total Cost of Ownership (TCO) and creating a higher efficiency of public spending, which in turn frees up resources to be redirected toward innovation and solving domain-specific challenges. Furthermore, this approach enhances interoperability, enabling greater cross-jurisdictional compatibility and simpler, more secure data and service exchange across all administrative and sectoral layers. The use of consistent models and processes also streamlines security, audits, and regulatory adherence, such as for GDPR and NIS2, which builds a foundation of quality and trust, resulting in more reliable public services. Finally, these elements combine to accelerate market innovation; predictable APIs and reusable data/AI products create a stable platform that significantly shortens the time-to-market for SMEs, startups, and vendors across every industry.

Principle 4: User-centricity

"Start from needs, not from systems."

Rationale. The customer is the central element in the creation of digital services. An in-depth understanding of the user's context, needs, and reasons why they choose or avoid a service is essential for creating solutions that are valuable and useful to users.

Description. The focus of the development of digital solutions for public administration is the provision of digital services to citizens, businesses, or any administrative institution, including those outside the country's borders, covering different types of cooperation (A2A, A2B, A2C). The development of digital solutions cannot be a goal by itself; the priorities and needs of digital services users must be clearly identified and addressed. Therefore, as far as possible, user needs and requirements should guide the design and development of public services.

Digital services must be inclusive, accessible and useful for all. All customers, regardless of their capabilities, location, or circumstances, should have equal access to and use of the solutions and services offered. It must be ensured that no group in society is excluded from the development and benefits offered by technology and public administration initiatives.

Implications. Service design becomes inherently driven by continuous user research and validation, making a shift from provider-oriented to citizen-oriented digital public services. Such user-centric approach requires that digital services are aligned with the typical life-events of citizens and integrated between different service providers. Furthermore, digital service providers must not only understand user diversity and comply with all relevant legislation and standards but also implement robust feedback mechanisms to facilitate ongoing improvement. The entire service delivery framework must support multi-channel service delivery , single contact points and a "no wrong door" approach, which guarantees that users can access assistance seamlessly through any channel, with their requests routed to the appropriate service or authority.

Principle 5: Connected and effortless public services

"Simpler is stronger."

Rationale. In a digital and interconnected public sector, simplification goes beyond reducing paperwork. It streamlines processes, eliminates duplication, connects systems, and makes services easier to access and maintain. Interoperability is a key enabler in this process, allowing data, systems, and organisations to work seamlessly together. It reduces administrative friction, speeds up service delivery, and lowers burdens on citizens and businesses. It also enhances clarity, accountability, and ultimately enables trust in digital public services.

Description. Administrative simplification should be guided by three concepts: digital first and streamlined processes, interoperable by design, and integrated and sustainable delivery of public services. Public administrations should prioritise digital channels for enabling access and use to public services and maintain inclusivity under the "no wrong – door" approach. The key to streamlining processes in public administration is the removal of redundant steps, the automation of tasks, and a focus on ensuring every action adds clear public value. Interoperability should be embedded from the outset across legal, organisational, semantic, and technical layers. This means using shared data models, common standards, and reusable components. Interoperable-by-design ensures services are connected, scalable, and capable of supporting integrated, cross-domain, and cross-border delivery. Simplified public services should form part of an integrated service ecosystem, where administrations collaborate across sectors and borders to offer seamless, user-oriented access. Integration depends on interoperable infrastructures, shared governance, and sustainable resource planning to ensure consistent quality and avoid duplication.

Implications. When administrative simplification is grounded in interoperability, it significantly reduces administrative costs and effort for users through clearer guidance and streamlined processes, making compliance with obligations more straightforward. This connected foundation directly improves service quality and speed by enabling system integration and process automation. These clear, consistent, and well-governed processes build a stronger, more trustworthy relationship between citizens and their public services.

Principle 6: Established standards and common specifications

"Prefer the well-trodden path."

Rationale. Public administrations have developed national technical specifications for interoperability, including extensions to API specifications and metadata definitions. However, these specifications often create silos in the cross-border context, as they are not necessarily compatible with each other. The emergence of data ecosystems, such as data spaces, has underscored the need for interoperability among ecosystem participants and, in the future, also between different ecosystems through federation capabilities based on global standards. These developments are universal and affect all sectors, as well as the exchange of data across sectors and business domains. It is no longer sufficient to allow technical specifications to be defined solely at the national level. Increasing the use of established standards and common specifications will benefit EU member states in the long run.

Description. This principle suggests that public administrations should adhere to established standards and common specifications – often first adopted by the private sector – and avoid creating their own or selecting those that are not widely adopted. Existing national and EU-level information systems should be gradually transitioned to applying standards and common specifications, if they are not doing so yet.

Member States must exchange information on the implementation of agreed standards and specifications and report any challenges they encounter in applying them. Where national extensions are necessary, these must be clearly documented and designed to remain interoperable with the core specification. Sharing open-source implementations of both core standards and their national extensions is encouraged, as this helps reduce implementation and maintenance efforts across Member States.

To promote consistent use and reuse, commonly adopted standards and specifications should be shared and maintained on the Interoperable Europe Portal. This enables Member States to reference existing solutions when updating or developing national information systems and supports greater alignment across Europe.

Implications. Using established standards and common specifications saves national resources, facilitates the development of cross-border digital services, and encourages greater collaboration among public administrations in various countries. Improved technical interoperability enhances the creation of European data spaces and other data ecosystems. When organisations design their infrastructure to be "interoperable by default", they are better prepared to utilise it for new applications.

Principle 7: Readiness for interoperability as a conditionality

"No interoperability, no funding."

Rationale. Interoperability is most effective and sustainable when designed into systems from the beginning. Building readiness upfront avoids costly retrofitting and ensures that public investments contribute to a connected European digital ecosystem. Linking interoperability-readiness to funding and procurement incentivises administrations to develop systems that can be smoothly integrated as new cross-border or cross-sector opportunities arise.

Description. The EIF promotes interoperability-readiness as a design and funding conditionality: systems must be built so that they can interoperate easily when a concrete, value-adding opportunity arises. The goal is not interoperability for its own sake, but

purposeful connections that deliver measurable public value. Each solution should publish its vocabularies, data models, APIs, and governance frameworks to allow future alignment and reuse. Administrations must demonstrate that new investments are technically and semantically ready to connect across ecosystems: "no interoperability, no funding" ensures that public money is spent only on systems designed for long-term interoperability.

Implications. Creates a culture of interoperability-by-design across public administrations, reducing future integration costs and avoiding fragmented systems. Ensures that every publicly funded IT solution contributes to the European interoperability through efficient development of public digital services utilising different data sources, data ecosystems and data spaces, and strengthening accountability in how digital investments deliver shared value.

Principle 8: In synergy with EU values and legislation

"Align once, implement many times."

Rationale. Interoperability must strengthen, not duplicate or contradict, the existing EU legal framework and fundamental values.

Description. The framework has been developed with close attention to alignment between its principles and recommendations and key European legislation (such as the GDPR, AI Act, NIS2, Data Governance Act and Interoperable Europe Act) while upholding EU values of transparency, openness, privacy, inclusion, and sustainability. In the same way, it is also recommended to follow a digital-ready policy-making approach in general and the practice of interoperability assessments in particular as one way of bridging the legal obligations and their practical implementation. In doing so, adherence not only with the existing legal framework and fundamental values could be promoted, but digital implementation would be considered from the beginning and thereby promote principles 1 (Subsidiarity and proportionality), 2 (transparent by design) and 4 (user centricity) of this framework. Moreover, conducting interoperability assessments in particular could help to ensure that solutions are being reused to foster interoperability, either specific to these legal obligations or specific to the context of the digital public service, in line with principle 3 (efficiency through re-use) and 6 (Established standards and common specifications) of this framework.) of this framework.

Implications. Creates coherence across EU digital policies, reduces compliance effort, and ensures that interoperability advances European rights, security, and sustainability objectives.

Principle 9: Data agency / EU data sovereignty

"The ability to make decisions and act independently in the digital domain"

Rationale. There is a growing concern that citizens, businesses, and public authorities in Member States are gradually losing control over data, as well as their capacity to innovate and effectively enforce legislation in the digital environment. The cloud delivery model used by many ICT providers remains heavily concentrated among a few large global actors in the United States and Asia, limiting diversity and strategic autonomy in the market.

Public Digital Services must be delivered in compliance with EU values, data protection laws and must be protected from regulatory shifts outside of European control and geopolitical shifts that could threaten the continuity of public services relying on private services operated and controlled outside the EU.

Even inside the EU vendor lock-in can constrain administrations' ability to re-use data, implement new functionalities in a cost-effective way and expose them to long term economic risks, with little possibility to mitigate.

Description. Ensure that public digital services are designed, built, and operated in ways that maintain the service providers' full agency — the ability to access and reuse its own data, to move applications between platforms, to choose between more vendors for development and maintain applications and in general evolve digital capabilities without undue dependency on individual ICT providers.

Implications. Public administrations should ensure unrestricted access to their data, including maintaining local backups where necessary. They should prioritise the use of open protocols that have multiple implementations, ideally including at least one actively maintained open-source option. Software developed with public funding should be released under terms that enable reuse and sharing across administrations.

Procurement and contract design should include risk-based exit strategies to ensure continuity and flexibility in case of vendor lock-in or changing service conditions. ICT suppliers should be evaluated for their long-term alignment with EU values, regulatory requirements, and digital sovereignty objectives.

Administrations should also strengthen their internal digital competence to retain ownership of key service logic, data models, and integration frameworks. Adequate procedures and resources should be established to enable the re-deployment of ICT applications on alternative platforms and with alternative service providers when needed.

Principle 10: Trustworthiness

"Security, privacy and trust enable interoperability, and vice-versa."

Rationale. Trust, security & privacy by design must be integrated safeguards throughout lifecycle of digital service. Security and privacy are key enablers for building digital public services with trust and reinforce security and privacy obligations in the context of EU-wide interoperable public services.

Description. Digital services and solutions must be designed to be reliable, secure, and protect user privacy. Security and trust are the foundation of public administrations, while respect for privacy strengthens user confidence and engagement. In the context of interoperability, accessibility of digital services regardless of time and location is an essential element.

Citizens and businesses must be confident that their interactions with public authorities take place in a secure and trustworthy environment that fully complies with regulatory requirements. Authorities must ensure the privacy of citizens and the confidentiality, authenticity, integrity, and irrevocability of the information provided by citizens and businesses. Customers must feel secure when using any digital service.

Implications. Digital service providers must create solutions that respect user data and ensure that information is available and protected against risks. They must also ensure the

service remains available, stable, and consistent for users across different locations, time zones, and times of use. It is important to plan maintenance during predictable periods of downtime and provide users with clear advance notice.

Principle 11: Assess, improve, deliver

"Measure what matters, then iterate."

Rationale. Regular assessments of the effectiveness and efficiency of interoperable public services ensure that these services deliver tangible value to citizens, businesses, and administrations. Such evaluations should be embedded in a continuous feedback loop that supports ongoing improvement. This involves selecting interoperable solutions before implementation based on their effectiveness, scalability, and suitability for purpose; monitoring performance during implementation to gather operational insights; and making evidence-based adjustments in response to feedback to optimise outcomes and ensure sustained service quality. Clear assessment metrics and communication enhance transparency, accountability, builds trust, and increases buy-in from users and stakeholders.

Description. To assess the effectiveness and efficiency of interoperable public services, public administrations can consider multiple dimensions, including service performance, costs, user satisfaction, flexibility, simplification, administrative burden, transparency, and reusability. Metrics and monitoring mechanisms should be integrated into service design from the outset, enabling continuous feedback and improvement.

Public administrations across the EU should aim to adopt common metrics for measuring efficiency and effectiveness to increase transparency and demonstrate the positive impact of interoperable public services.

Implications. Regular assessment of the effectiveness and efficiency of interoperable public services helps optimise the use of resources by identifying high-value investments and eliminating redundant or costly processes. It enhances service quality through continuous monitoring, performance evaluation, and the ongoing improvement of interoperable systems. Such assessments also strengthen transparency and trust by providing clear evidence of service outcomes and efficiency gains. Moreover, they support the development of integrated and scalable services by validating solutions that are interoperable, reusable, and adaptable across borders and sectors.

Principle 12: AI for interoperability and interoperability for AI

"AI should connect systems, even the ones that use AI."

Rationale. The rapid integration of Artificial Intelligence (AI) into public administration creates both an opportunity and a necessity for rethinking interoperability and the methods for reaching it. On one side, AI can vastly improve the capacity of systems to exchange, interpret, and reuse information across legal, organisational, semantic, or technical boundaries. On the other hand, the growing diversity of AI tools, data, and governance models, risks producing new silos and incompatibilities between public sector organisations and member states. Therefore, this principle is needed to ensure that AI becomes a driver for interoperability rather than a new barrier—helping achieve seamless cooperation across the European public sector while safeguarding coherence, trust, and compliance with shared standards.

Description. This principle establishes that AI adoption must both enable and drive conformance to interoperability requirements, as defined in the European Interoperability Framework. It calls for the use of AI technologies, such as Symbolic AI, Machine Learning, Generative AI and agentic AI, to strengthen cross-border and cross-domain interoperability. At the same time, it requires that AI systems themselves are designed to interoperate, adhere to common standards, transparent data structures, explainable algorithms, and other ethical requirements under relevant EU legislation. In essence, it positions AI as a core enabler and a compliant participant within the ecosystem of interoperable digital public services.

Implication. Embedding this principle across the EU public sector will generate tangible benefits for citizens, businesses, and administrations. Citizens will experience simpler, faster, and more personalised services that anticipate their needs and function seamlessly across borders. Businesses will gain from reduced administrative burden, improved data access, and consistent AI-enabled procedures in different Member States. Public administrations will benefit from enhanced efficiency, data-driven insight, and shared innovation capacity, as AI solutions become interoperable and reusable across domains.

4. Recommendations

This chapter presents the recommendations of the EIF under each of the four application scenarios as introduced in Chapter 2:

- Interoperability in **Legislation Drafting**
- Interoperability in **Policy Formulation**
- Interoperability in **Service Design and Delivery**
- **Developing** interoperability solutions

All the above application scenarios include recommendations that can also be connected to one or more of the four interoperability layers (Legal, Organisational, Semantic or Technical Interoperability). Moreover, some cross-cutting requirements are grouped under the Interoperability Governance layer.

So, every recommendation includes, apart from the main **description** of what needs to be done or achieved, the following information:

- Its **nature**, which is further characterised as:
  - **Mandatory**, which means meeting that recommendation is essential, in order to claim conformance with the EIF.
  - **Optional**, which indicates a recommendation that contributes to interoperability but could be left unmet or could be met with some other way, in a given situation.
  - **Tentative**, which indicates a recommendation that is not yet mature, to be included as optional or mandatory.
- The main **stakeholder roles** that should are affected and should contribute in meeting the recommendation.
- The relevant **interoperability layer.**
- The relevant **principle.**
- The **relevant legislation**, if any, that should be consulted when working towards the recommendation.
- Examples of **relevant Interoperable Europe (IE) solutions** that should be reused in achieving the recommendation.

Each sub-chapter begins with a summary table providing an overview of the recommendations for the respective application scenario, followed by a detailed description of each recommendation.

4.1 Interoperability in Legislation Drafting

Table 3: Summary of Recommendations for Legislation drafting scenario

Rec #	Recommendation	Main stakeholder roles	IoP Layers	EIF Principles	Relevant legislation	Relevant IoP Solutions
RC1.1	Embed Interoperability-by-Design in Legislation	Legislators	All	7 - Readiness for interoperability as a conditionality	Interoperable Europe Act	
RC1.2	Integrate Interoperability Impact Assessments Throughout the Legislative Lifecycle	Legislators, policy makers	All	7 – Readiness for interoperability as a conditionality; 8 – In synergy with EU values and legislation; 11 – Assess, improve, deliver	Interoperable Europe Act	Interoperability Assessment Guidelines; Interoperability Assessment Tool (on Interoperable Europe Portal)
RC1.3	Ensure digital transparency and structured publication of legislation	Legislators, Policy makers, ICT providers, Public service providers	Legal, semantic, technical	2–Transparency by design; 6 – Established standards and common specifications	Open Data Directive	LEOS, ELI, ELI-DL
RC1.4	Reference and Promote Interoperability Frameworks and Solutions	Legislators, Policy makers, Standardisation bodies, Public service providers	All	3 – Efficiency through reuse; 6 – Established standards and common specifications	Interoperable Europe Act	EIF, EIRA, Catalogue of Interoperability Solutions; Catalogue of Interoperable Europe Solutions (Interoperable Europe Portal)
RC1.5	Establish Regulatory Sandboxes for Interoperability Testing	Legislators, ICT providers, Public service providers	All		Interoperable Europe Act	
RC1.6	Use Common Legal and Data Vocabularies and Ontologies	Legislators, ICT providers,	Semantic, legal	3 – Efficiency through reuse; 6 – Established standards and common specifications		EU Core Vocabularies, DCAT-AP
RC1.7	Include clauses enabling data sharing and re-use	Legislators, Policy makers	Legal, organisational	3 – Efficiency through reuse	Data Governance Act, Open	

Rec #	Recommendation	Main stakeholder roles	IoP Layers	EIF Principles	Relevant legislation	Relevant IoP Solutions
					Data Directive	
RC1.8	Establish legal identifiers and electronic recognition mechanisms	Legislators, ICT providers, Public service providers	Legal, technical, organisational	5 – Connected and effortless public services	eIDAS; European Digital Identity Framework	
RC1.9	Strengthen participatory processes	Legislators, Service desginers, public service providers	Legal, organisational	4 – User-centricity; 11 – Assess, improve, deliver		EUSurvey
RC1.10	Leverage AI for consistent legal drafting	Legislators, ICT providers	Legal, semantic, technical	13 – AI for interoperability and interoperability for AI	EU AI Act	
RC1.11	Reuse model clauses and modular legislation patterns	Legislators	Legal, semantic	3 – Efficiency through reuse		
RC1.12	Enable multilingual semantic alignment	Legislators, policy makers,	Semantic, technical	4 – User-centricity; 13 – AI for interoperability and interoperability for AI		

RC1.1 Embed Interoperability-by-Design in Legislation

Legislators should consider interoperability principles and requirements from the outset of the legislative process to ensure coherent, efficient, and trusted public services. This process should consider interoperability across legal, organisational, semantic, and technical layers when drafting or revising legal acts. Legislators, legal services, and digital-government units share responsibility for ensuring this alignment. Practical tools such as interoperability-by-design checklists and legislative impact clauses should guide drafting, while compliance can be tested by reviewing draft acts for interoperability clauses. Policy makers can support this process with analytical input, while public service providers can highlight operational implications.

Nature: Mandatory
Stakeholder Roles: Legislators
EIF Principle: 7 – Readiness for interoperability as a conditionality
IoP Layer: All

Relevant Legislation: Interoperable Europe Act (EU) 2024/903
Relevant IE Solution: --

RC1.2 Integrate Interoperability Impact Assessments Throughout the Legislative Lifecycle

When developing or revising legislation that affects trans-European public services, legislators should conduct an interoperability assessment in line with the binding requirements of the Interoperable Europe Act. This assessment should identify whether proposed requirements facilitate or hinder data exchange, system compatibility, and cross-border cooperation. Legislators should also introduce explicit checkpoints (ex-ante, mid-term, ex-post) to assess interoperability impact during drafting and enforcement. Impact assessment templates can facilitate the process. Policy makers Policy makers should set clear rules and standards to ensure transparency, interoperability, and coordination across institutions oversee implementaiton and can support the assessments by providing analytical evidence. Public service providers should contribute operational feedback on implementation feasibility.

Nature: Mandatory
Stakeholder Roles: Legislators, policy makers
EIF Principle: 7 – Readiness for interoperability as a conditionality ; 8 – In synergy with EU values and legislation; 11 – Assess, improve, deliver
IoP Layer: All
Relevant Legislation: Interoperable Europe Act
Relevant IE Solution: Interoperability Assessment Guidelines; Interoperability Assessment Tool (on Interoperable Europe Portal)

RC1.3 Ensure digital transparency and structured publication of legislation

Legislative drafting and publication should be digital-ready and transparent by design, using interoperable, machine-readable formats and open drafting tools. Drafting processes must capture structured metadata, versioning, explanatory context, and information on data sources or potential algorithmic impacts of automated decision-making laws to ensure traceability and reuse.

For implementation, machine-readable formats such as XML, RDF, or JSON-LD following linked-data principles can be used. Policy Makers responsible for digital government and

interoperability should establish governance frameworks and procedures to promote transparency and machine-readability. They should also facilitate coordination across ministries, national parliaments, and EU institutions to promote common practices for open legislative data. ICT providers must deliver open, auditable, and secure systems that support drafting, reviewing, and publishing legal texts, maintain structured metadata, and ensure version control. Official journals and ICT agencies are responsible for implementation and testing, including verification of machine-readable metadata and interlinking of legal content.

These efforts can be further enhanced by considering the development of a metadata layer to connect EU and national legislation to enable automatic alignment of definitions and obligations. Such a metadata layer could be implemented using ELI extensions and legislative graph APIs, with testing to confirm successful cross-linking.

Nature: Mandatory
Stakeholder Roles: Legislators, Policy makers, ICT providers, Public service providers
EIF Principle: 2 – Transparency by design; 6 – Established standards and common specifications
IoP Layer: Legal, semantic, technical
Relevant Legislation: Directive (EU) 2019/1024 (Open Data Directive)
Relevant IE Solution: LEOS, ELI, ELI-DL

RC1.4 Reference and Promote Interoperability Frameworks and Solutions

Whenever laws address data exchange or information systems, they should cite recognized interoperability frameworks and solutions. Legal drafters, ICT ministries, and standardisation bodies are responsible for ensuring compliance.
Legislators should also promote the reuse and openness of interoperability solutions by referencing existing catalogues, such as the European Commission's Catalogue of Interoperability Solutions, including those labelled as Interoperable Europe Solutions. Where possible, legislation should require that new solutions be openly available, for example via the Interoperable Europe Portal, to ensure transparency, prevent duplication, and support alignment across Member States.

Nature: Mandatory
Stakeholder Roles: Legislators, Policy makers, Standardisation bodies, Public service providers

EIF Principle: 3 – Efficiency through reuse; 6 – Established standards and common specifications
IoP Layer: Legal
Relevant Legislation: Interoperable Europe Act
Relevant IE Solution: EIF, EIRA, Catalogue of Interoperability Solutions; Catalogue of Interoperable Europe Solutions (Interoperable Europe Portal)

RC1.5 Establish Regulatory Sandboxes for Interoperability Testing

Legislators can create a favorable legal framework to enable regulatory sandboxes, allowing stakeholders to test innovative digital and interoperable solutions in a controlled environment. These sandboxes help identify challenges early, supporting adaptive law-making and evidence-based refinement of interoperability requirements. Regulatory innovation offices and relevant ministries oversee implementation. Sandbox charters and evaluation protocols can support implementation. Testing compares outcomes under experimental rules versus standard rules.

Nature: Optional
Stakeholder Roles: Legislators, ICT providers, Public service providers
EIF Principle: --
IoP Layer: Legal, Technical
Relevant Legislation: Interoperable Europe Act
Relevant IE Solution: --

RC1.6 Use Common Legal and Data Vocabularies and Ontologies

Legislation should adopt harmonised terminologies and reference data models to ensure semantic consistency across Member States. Sectoral ontologies should map legal concepts across domains such as health, environment, and justice to prevent semantic drift. Legal drafters, domain authorities, semantic boards, and data architects are responsible. Solutions that support practical implementation include: EU Core Vocabularies (Person, Organisation, Location), DCAT-AP, interoperability knowledge graphs, and alignment registries. Testing can include AI-based semantic validation and verification of aligned definitions.

Nature: Optional
Stakeholder Roles: Legislators, ICT providers

EIF Principle: 3 – Efficiency through reuse; 6 – Established standards and common specifications
IoP Layer: Legal, Semantic
Relevant Legislation: --
Relevant IE Solution: EU Core Vocabularies, DCAT-AP

RC1.7 Include clauses enabling data sharing and re-use

Laws should explicitly authorise lawful data sharing and re-use, providing clear legal bases. Legislators, data-protection authorities, and open-data offices share this responsibility. Implementation employs model clauses from the Data Governance Act and Open Data Directive.

Nature: Mandatory
Stakeholder Roles: Legislators, Policy makers
EIF Principle: 3 – Efficiency through reuse
IoP Layer: Legal, organisational
Relevant Legislation: Data Governance Act, Open Data Directive
Relevant IE Solution: --

RC1.8 Establish legal identifiers and electronic recognition mechanisms

Every law should ensure the recognition of electronic identities, documents, and administrative acts across borders. Ministries of justice, identity providers, and interoperability authorities are responsible. Implementation builds on the European Digital Identity Wallet and trust-service standards. Tests involve cross-border validation. Example: the eIDAS Regulation ensuring mutual recognition of eIDs.

Nature: Mandatory
Stakeholder Roles: Legislators, ICT providers, Public service providers
EIF Principle: 5 – Connected and effortless public services
IoP Layer: Legal, technical, organisational
Relevant Legislation: eIDAS (EU) 910/2014; European Digital Identity Framework (EU) 2024/1184
Relevant IE Solution: --

RC1.9 Strengthen participatory processes

Legislators should engage stakeholders (citizens, businesses, experts) early to understand interoperability needs. Co-creation mechanisms and structured consultations can inform drafting decisions, ensuring that legal provisions are conceived and adapted to effectively meet stakeholder needs. Parliaments and ministries convene and coordinate such participatory processes. Citizens, businesses, and academia, as relevant for specific legal initiatives, are active participants in the co-creation or consultative processes. Digital participation platforms can facilitate implementation. The outcomes can be tested based on engagement levels and reporting on how feedback is taken into account.

Nature: Mandatory
Stakeholder Roles: Legislators, Service designers, public service providers
EIF Principle: 4 – User-centricity; 11 – Assess, improve, deliver
IoP Layer: Legal, organisational
Relevant Legislation: --
Relevant IE Solution: EUSurvey

RC1.10 Leverage AI for consistent legal drafting

AI should support lawmaking by suggesting harmonised language, detecting inconsistencies, and improving multilingual alignment. This is negotiable but recommended. Parliamentary drafting offices and legal-informatics centres are involved. Implementation integrates AI drafting assistants linked to legal ontologies. Testing might compare AI-generated and human-edited versions for consistency.

Nature: Tentative
Stakeholder Roles: Legislators, ICT providers
EIF Principle: 12 – AI for interoperability and interoperability for AI
IoP Layer: Legal, semantic, technical
Relevant Legislation: EU AI Act
Relevant IE Solution: --

RC1.11 Reuse model clauses and modular legislation patterns

Promote libraries of reusable, pre-approved clauses for data-sharing and interoperability to ensure consistency. Drafting offices and legal repositories manage them. Implementation uses digital clause libraries and AI drafting assistants. Testing measures clause reuse rates.

Nature: Mandatory
Stakeholder Roles: Legislators
EIF Principle: 3 – Efficiency through reuse
IoP Layer: Legal, semantic
Relevant Legislation: --
Relevant IE Solution: --

RC1.12 Enable multilingual semantic alignment

Ensure that translations preserve semantic equivalence using ontology-based tools. Translation centres and ontology curators manage it. Implementation uses multilingual legal ontologies and AI translation validation. Testing assesses semantic similarity across languages. Example: enriched eTranslation pipelines integrating legal concept mappings.

Nature: Optional
Stakeholder Roles: Legislators, policy makers
EIF Principle: 4 – User-centricity; 12 – AI for interoperability and interoperability for AI
IoP Layer: Semantic, technical
Relevant Legislation:
Relevant IE Solution:

4.2 Interoperability in Policy Formulation

Table 4: Summary of Recommendations for Policy formulation Scenario

Rec #	Recommendation	Main stakeholder Roles	IoP Layers	EIF Principles	Relevant Legislation	Relevant IoP Solutions
RC2.1	Integrate interoperability by design into policy formulation	Legislators, policy makers, service designers, ICT providers, public service providers	All	1 – Subsidiarity & proportionality; 5 – Connected & effortless public services; 6 – Common specifications; 7 – Readiness for interoperability	Interoperable Europe Act; Single Digital Gateway Regulation; Open Data Directive	Base Registries; EIRA; DCAT-AP
RC2.2	Apply evidence-based and data-driven policymaking	Policy makers, data stewards, ICT providers, standardisation bodies	Semantic, organisationa, technical	3 – Efficiency through reuse; 10 – Trustworthiness; 11 – Assess, improve, deliver; 12 –	Data Governance Act; Open Data Directive; AI Act; GDPR	EU Data Spaces; DCAT-AP; Base Registries; Interoperable

Rec #	Recommendation	Main stakeholder Roles	IoP Layers	EIF Principles	Relevant Legislation	Relevant IoP Solutions
				Preservation of information; 13 – AI for interoperability		Europe Portal
RC2.3	Ensure policy alignment across governance levels	Policy makers (local, regional, national, EU), intergovernment al units, standardisation bodies	Organisationa l, semantic	1 – Subsidiarity & proportionality	Interoperabl e Europe Act	
RC2.4	Use digital-twin and AI simulation tools for policy testing	Policy makers, ICT providers, innovation hubs	Technical, semantic	13 – AI for interoperability and interoperability for AI		
RC2.5	Establish cross-sector interoperability boards for coherence	Legislators, senior policy makers	Organisationa l	8 – In synergy with EU values and legislation	Interoperabl e Europe Act	
RC2.6	Integrate interoperability into policy impact assessments	Policy makers, analysts, legislative drafters	Legal, organisational	11 – Assess, improve, deliver	Interoperabl e Europe Act	
RC2.7	Promote the re-use of interoperable policy models	Policy designers, public administrations, standardisation bodies	Organisationa l, semantic, technical	3 – Efficiency through reuse	Interoperabl e Europe Act	Interoperable Europe Portal
RC2.8	Apply AI-assisted policy analysis and coherence checking	Policy makers, legal informatics experts, ICT providers	Semantic, technical	13 – AI for interoperability and interoperability for AI	AI Act	
RC2.9	Maintain an interoperable policy knowledge base	Policy documentation offices, ICT providers, data stewards	Semantic, technical	2 – Transparent by design	Open Data Directive	
RC2.10	Connect policy cycles to feedback and monitoring loops	Policy makers, public service providers, service designers	Organisationa l, technical	11 – Assess, improve, deliver		eGovernmen t Benchmark; NIFO dashboards; Repository of good practices (Interoperabl e Europe Portal)
RC2.11	Build a community of practice and co-creation for	Policy makers, legislators, academia, ICT providers, civil society	Organisationa l, semantic	2 – Transparent by design; 4 – User-centricity; 8 – In synergy	Interoperabl e Europe Act; Open Data Directive;	Interoperable Europe Community; Interoperable Europe

Rec #	Recommendation	Main stakeholder Roles	IoP Layers	EIF Principles	Relevant Legislation	Relevant IoP Solutions
	interoperable policymaking			with EU values and legislation	Data Governance Act; GDPR	Portal; DCAT-AP; Base Registries
RC2.12	Enable common government capability models	Legislators, policy makers, public service providers	Organisational, technical	5 – Connected and effortless public services		EIRA

RC2.1 Integrate interoperability by design into policy formulation

Legislators and policy makers should ensure interoperability is embedded throughout the policy cycle - from concept to implementation. Interoperability requirements must guide legal drafting, policy objectives, and operational planning, enabling data exchange, service reuse, and cross-border compatibility. Service designers and ICT providers must use EIF-aligned frameworks and assess interoperability impacts early. Public service providers should remove barriers to data sharing and align processes with EU interoperability standards. Embedding interoperability by design guarantees that new policies are legally coherent, technologically feasible, and ready for implementation across jurisdictions.

Nature: Mandatory
Stakeholder Roles: Legislators, policy makers, service designers, ICT providers, public service providers
EIF Principle: 1 – Subsidiarity & proportionality; 5 – Connected & effortless public services; 6 – Common specifications; 7 – Readiness for interoperability
IoP Layer: All
Relevant Legislation: Interoperable Europe Act; Single Digital Gateway Regulation; Open Data Directive
Relevant IE Solution: Base Registries; EIRA; DCAT-AP

RC2.2 Apply evidence-based and data-driven policymaking

Policy makers should base decisions on harmonised, high-quality, and interoperable data from shared data spaces. Data stewards and ICT providers must ensure data provenance, explainability, and algorithmic transparency, particularly in AI-supported analytics. Standardisation bodies should promote common data models and linked indicators for comparability. This enables an adaptive policy lifecycle in which evidence informs every stage, ensuring continuous improvement, transparency, and accountability in line with EU values and digital governance frameworks.

Nature: Mandatory
Stakeholder Roles: Policymakers
EIF Principle: 3 – Efficiency through reuse; 10 – Trustworthiness; 11 – Assess, improve, deliver; 12 – Preservation of information; 12 – AI for interoperability
IoP Layer: Semantic, organisational, technical
Relevant Legislation: Data Governance Act; Open Data Directive; AI Act; GDPR
Relevant IE Solution: EU Data Spaces; DCAT-AP; Base Registries; Interoperable Europe Portal

RC2.3 Ensure policy alignment across governance levels

Policy makers at all levels - local, regional, national, and EU - should coordinate through shared interoperability architectures to ensure coherent, non-duplicative policymaking. Intergovernmental units must align priorities, indicators, and processes through common frameworks and dashboards. Standardisation bodies can support this alignment by defining reference models and terminologies. Consistent governance across levels prevents fragmentation, strengthens subsidiary, and ensures that interoperability is maintained as policies scale across administrative boundaries.

Nature: Optional
Stakeholder Roles: Policy makers (local, regional, national, EU), intergovernmental units, standardisation bodies
EIF Principle: 1 – Subsidiarity and proportionality
IoP Layer: Organisational, semantic
Relevant Legislation: Interoperable Europe Act
Relevant IE Solution: --

RC2.4 Use digital-twin and AI simulation tools for policy testing

Policy makers should adopt digital twins and AI-based simulation environments to test potential policy outcomes before formal adoption. ICT providers and innovation hubs can co-develop tools that combine interoperable datasets and predictive models to visualise policy impacts. This proactive, data-driven approach enhances foresight, reduces risks, and improves coordination between policy options and implementation realities, particularly in complex or high-impact sectors such as environment, health, and mobility.

Nature: Tentative

Stakeholder Roles: Policy makers, ICT providers, innovation hubs
EIF Principle: 12 – AI for interoperability and interoperability for AI
IoP Layer: Technical, semantic
Relevant Legislation: --
Relevant IE Solution: --

RC2.5 Establish cross-sector interoperability boards for coherence

Legislators and senior policy makers should institutionalise permanent interoperability boards to coordinate across policy areas such as health, environment, and justice. These boards, framed by the Better Regulation agenda, should facilitate horizontal governance, ensure consistent terminology, and harmonise data-sharing practices. Cross-sector coordination strengthens policy coherence, supports integrated service delivery, and promotes accountability across government departments and levels.

Nature: Optional
Stakeholder Roles: Legislators, senior policy makers
EIF Principle: 8 – In synergy with EU values and legislation
IoP Layer: Organisational
Relevant Legislation: Interoperable Europe Act
Relevant IE Solution: --

RC2.6 Integrate interoperability into policy impact assessments

Policy makers and analysts should include interoperability as a mandatory dimension in all regulatory and policy impact assessments. Using EIF-aligned templates, they should assess how proposed measures affect data sharing, service integration, and administrative collaboration. Legislative drafters must ensure that interoperability requirements are clearly articulated in the legal text. This practice institutionalises interoperability as a measurable performance criterion in the Better Regulation toolbox.

Nature: Mandatory
Stakeholder Roles: Policy makers, analysts, legislative drafters
EIF Principle: 11 – Assess, improve, deliver
IoP Layer: Legal, organisational
Relevant Legislation: Interoperable Europe Act
Relevant IE Solution:

RC2.7 Promote the re-use of interoperable policy models

Policy designers should document and publish interoperable policy models as open, reusable templates. Public administrations can adapt and replicate these models to avoid redundant work and accelerate service delivery. Standardisation bodies should curate and maintain repositories of validated policy models that reflect EU and national best practices. This reuse culture enhances efficiency, ensures coherence, and encourages innovation through shared learning.

Nature: Tentative
Stakeholder Roles: Policy designers, public administrations, standardisation bodies
EIF Principle: 3 – Efficiency through reuse
IoP Layer: Organisational, semantic, technical
Relevant Legislation: Interoperable Europe Act
Relevant IE Solution: Interoperable Europe Portal

RC2.8 Apply AI-assisted policy analysis and coherence checking

Policy makers and legal informatics experts should employ AI-enabled tools to analyse legislative and policy texts, identifying overlaps, gaps, and inconsistencies. ICT providers can develop semantic reasoning systems and ontologies to support these analyses. Automating coherence checks improves legislative quality, reduces duplication, and enhances regulatory transparency across jurisdictions.

Nature: Tentative
Stakeholder Roles: Policymakers, ICT Providers
EIF Principle: 12 – AI for interoperability and interoperability for AI
IoP Layer: Semantic, technical
Relevant Legislation: AI Act
Relevant IE Solution: --

RC2.9 Maintain an interoperable policy knowledge base

Policy documentation offices should maintain interoperable repositories linking policies, laws, indicators, and evaluations. ICT providers and data stewards must ensure these repositories follow open data and metadata standards, enabling discoverability, transparency, and cross-domain analysis. Such knowledge bases create institutional

memory and strengthen evidence-based governance by connecting data, law, and policy in a unified framework.

Nature: Tentative
Stakeholder Roles: Policy documentation offices, ICT providers, data stewards
EIF Principle: 2 – Transparent by design
IoP Layer: Semantic, technical
Relevant Legislation: Open Data Directive
Relevant IE Solution: --

RC2.10 Connect policy cycles to feedback and monitoring loops

Policy makers should integrate continuous monitoring and feedback mechanisms into policy cycles. Public service providers should collect performance data and user feedback, while service designers should translate insights into service improvements. Through interoperable dashboards and APIs, results can be shared in real time, ensuring transparent evaluation and adaptive policymaking that continuously improves policy outcomes.

Nature: Optional
Stakeholder Roles: Policy makers, public service providers, service designers
EIF Principle: 11 – Assess, improve, deliver
IoP Layer: Organisational, technical
Relevant Legislation: --
Relevant IE Solution: eGovernment Benchmark; NIFO dashboards; Repository of good practices (Interoperable Europe Portal)

RC2.11 Build a community of practice and co-creation for interoperable policymaking

Policy makers and legislators should actively participate in EU-wide interoperability communities to exchange best practices and co-create policies. Academia, ICT providers, and civil society should be engaged as equal partners in co-design processes to ensure transparency and inclusiveness. Collaborative governance fosters trust, ensures user-centred policies, and accelerates the harmonisation and deployment of interoperable public services across member states.

Nature: Optional

Stakeholder Roles: Policy makers, legislators, academia, ICT providers, civil society

EIF Principle: 2 – Transparent by design; 4 – User-centricity; 8 – In synergy with EU values and legislation

IoP Layer: Organisational, semantic

Relevant Legislation: Interoperable Europe Act; Open Data Directive; Data Governance Act; GDPR

Relevant IE Solution: Interoperable Europe Community; Interoperable Europe Portal; DCAT-AP; Base Registries

RC2.12 Enable common government capability models

Legislators and policy makers should establish and maintain common capability models that define shared functions, services, and processes across public administrations. Public service providers can use these models to harmonise operations. These models reduce duplication, clarify institutional roles, and underpin interoperability by aligning organisational capabilities across government.

Nature: Optional

Stakeholder Roles: Legislators, policy makers, public service providers

EIF Principle: 5 – Connected and effortless public services

IoP Layer: Organisational, technical

Relevant Legislation: --

Relevant IE Solution: EIRA

4.3 Interoperability in Service Design and Delivery

Table 5: Summary of Recommendations for Service design and delivery Scenario

Rec #	Recommendation	Stakeholders	IoP Layers	EIF Principles	Relevant legislation	Relevant IoP Solutions
RC3.1	Design services around users and life events	Public service providers, Service designers	Organisational, Semantic, Technical	4 – User-centricity	Single Digital Gateway Regulation (EU 2018/1724)	—
RC3.2	Adopt the once-only principle	Public service providers, Service designers, ICT providers, Data controllers, Privacy officers	Organisational, Semantic, Technical	5 – Connected and effortless public services	Interoperable Europe Act (EU 2024/903); GDPR (EU 2016/679)	Once-Only Technical System (OOTS)
RC3.3	Use shared interoperability building blocks	Public service providers, Service	Organisational, Semantic, Technical	6 – Established standards and	Interoperable Europe Act (EU 2024/903)	eID, eDelivery, eInvoicing

Rec #	Recommendation	Stakeholders	IoP Layers	EIF Principles	Relevant legislation	Relevant IoP Solutions
		designers, ICT providers		common specifications		
RC3.4	Map and reuse existing interoperability solutions	Public service providers, Service designers, ICT providers	Organisational, Semantic, Technical	3 – Efficiency through reuse	Open Data Directive (EU 2019/1024); Interoperable Europe Act (EU 2024/903)	All Interoperable Europe Solutions
RC3.5	Apply participatory design methods and collect feedback	Public service providers, Service designers, ICT providers	Organisational, Technical	4 – User-centricity	—	—
RC3.6	Leave no one behind (Accessibility)	Public service providers, Service designers, ICT providers	Technical	4 – User-centricity	European Accessibility Act (EU 2019/882); Web Accessibility Directive (EU 2016/2102)	WCAG 2.0
RC3.7	Implement interoperable service-integration layers	Public service providers, Service designers, ICT providers	Semantic, Technical	6 – Established standards and common specifications	Interoperable Europe Act (EU 2024/903)	EIRA
RC3.8	Adopt API-first and data space integration principles	Public service providers, Service designers, ICT providers	Semantic, Technical	9 – Data agency / EU data sovereignty	Data Act (EU 2023/2854); Data Governance Act (EU 2022/868)	—
RC3.9	Guarantee security and privacy across interoperable chains	Public service providers, Service designers, ICT providers	Technical	10 – Trustworthiness	NIS2 (EU 2022/2555); GDPR (EU 2016/679)	—
RC3.10	Ensure multilingual and cultural interoperability via AI	Public service providers, Service designers, ICT providers	Technical, Semantic	12 – AI for interoperability and interoperability for AI	—	eTranslation API
RC3.11	Introduce interoperability testbeds and sandboxes	Public service providers, Service designers, ICT providers	Technical	11 – Assess, improve, deliver	AI Act (EU 2024/1689)	—
RC3.12	Ensure service lifecycle management and continuous improvement	Public service providers, Service designers, ICT providers	All	11 – Assess, improve, deliver	—	—

Rec #	Recommendation	Stakeholders	IoP Layers	EIF Principles	Relevant legislation	Relevant IoP Solutions
RC3.13	Leverage AI for intelligent service personalisation	Public service providers, Service designers, ICT providers	Technical	12 – AI for interoperability and interoperability for AI	AI Act (EU 2024/1689)	—
RC3.14	Implement event-driven interoperability	Public service providers, Service designers, ICT providers	Technical, Semantic	5 – Connected and effortless public services	—	—
RC3.15	Foster cross-border and cross-sector service federation	Public service providers, Service designers, ICT providers	All	9 – Data agency / EU data sovereignty	eIDAS (EU 910/2014); European Digital Identity Framework (EU 2024/1184)	—
RC3.16	Establish metrics and monitoring for interoperable service performance	Public service providers, Service designers, ICT providers	All	11 – Assess, improve, deliver	Interoperable Europe Act (EU 2024/903)	eGovernment Benchmark
RC3.17	Integrate sustainability and green interoperability	Public service providers, Service designers, ICT providers	Technical	8 – In synergy with EU values and legislation	EU Green Deal framework	—

RC3.1 Design services around users and life events

Public services should be organised around citizens' and businesses' needs rather than administrative silos. This user-centric, life-event-based design is essential under the digital-by-default principle, requiring administrations to develop services using user journeys, personas, and feedback loops. Responsibility lies with service owners and UX teams, who must measure success through user satisfaction and usability benchmarks, as demonstrated in the Single Digital Gateway.

Nature: Mandatory
Stakeholder Roles: Public Service Providers, Service Designers
EIF Principle: 4 – User-centricity
IoP Layer: Organisational, semantic, technical
Relevant Legislation: Single Digital Gateway Regulation (EU 2018/1724)
Relevant IE Solution: --

RC3.2 Adopt the once-only principle

Administrations should collect data from users only once and reuse it securely across borders and domains. To deliver services that feel effortless to users, public administrations should integrate their back-end processes so that data can be reused rather than repeatedly requested. The information requested must be kept to a minimum, taking into account the need for efficiency and user convenience. Binding under the Interoperable Europe Act, this principle relies on base registries, consent management, and secure APIs to reduce duplication and burden. Data controllers and privacy officers ensure compliance with GDPR, while effectiveness is tested through measurable reductions in repeated data requests, as seen in the Once-Only Technical System (OOTS).

Nature: Mandatory
Stakeholder Roles: Organisational, semantic, technical
EIF Principle: 5 – Connected and effortless public services
IoP Layer: Organisational, semantic, technical
Relevant Legislation: Interoperable Europe Act (EU 2024/903); GDPR (EU 2016/679)
Relevant IE Solution: Once-Only Technical System (OOTS)

RC3.3 Use shared interoperability building blocks

Service developers must integrate common reusable components for identification, signatures, messaging, and semantics. This practice ensures consistency and efficiency across administrations, with ICT agencies adopting CEF Building Blocks such as eID, eDelivery, and eInvoicing. Conformance tests and integration audits demonstrate compliance, exemplified by their reuse in the Business Registers Interconnection System.

Nature: Optional
Stakeholder Roles: Public service providers, Service designers, ICT providers
EIF Principle: 6 – Established standards and common specifications
IoP Layer: Organisational, semantic, technical
Relevant Legislation: Interoperable Europe Act (EU 2024/903)
Relevant IE Solution: eID, eDelivery, eInvoicing

RC3.4 Map and reuse existing interoperability solutions

Before developing new systems, administrations should identify and reuse solutions available in the Catalogue of Interoperable Europe Solutions. This measure enhances

efficiency and avoids duplication. Solution owners document reuse, and monitoring focuses on adoption rates across Member States. A strong example is the reuse of ELI and DCAT-AP standards in national open-data portals.

Nature: Mandatory
Stakeholder Roles: Public service providers, Service designers, ICT providers
EIF Principle: 3 – Efficiency through reuse
IoP Layer: Organisational, semantic, technical
Relevant Legislation: Open Data Directive (EU 2019/1024); Interoperable Europe Act (EU 2024/903)
Relevant IE Solution: All Interoperable Europe Solutions

RC3.5 Apply participatory design methods and collect feedback

Citizens, businesses, and experts should actively participate in the co-design of services. This recommended approach brings transparency and inclusiveness to digital transformation, requiring service owners and civic-technology partners to conduct workshops and prototyping sessions. Impact is measured by participation rates and prototype adoption.

Provide mechanisms for collecting user feedback. Ensure that all users can share their experiences, report issues, and propose improvements to Digital Public Services through multiple channels, such as online forms, surveys, chatbots, or help desks. Collected input should be regularly analysed and used to inform service updates, design improvements, and policy decisions. Communicate back to users how their feedback has been addressed to build trust, transparency, and continuous improvement in service delivery.

Nature: Mandatory
Stakeholder Roles: Public service providers, Service designers, ICT providers
EIF Principle: 4 – User-centricity
IoP Layer: Organisational, technical
Relevant Legislation: --
Relevant IE Solution:--

RC3.6 Leave no one behind

Ensure that Digital Public Services are accessible to all citizens, including people with disabilities, older people, and other disadvantaged groups. Accessibility should cover both technical and content-related aspects, such as compliance with accessibility standards (e.g., WCAG), clear and inclusive language, and compatibility with assistive technologies. Accessibility must be embedded from the start of service design, following the Web Accessibility Directive and WCAG standards. Services should be designed to accommodate different devices, digital skills, and connectivity levels, ensuring equal access and participation for everyone, regardless of their physical, social, or economic situation. Compliance should be verified through accessibility audits and certification, ensuring full adherence to EU standards.

Nature: Mandatory
Stakeholder Roles: Public service providers, Service designers, ICT providers
EIF Principle: 4 – User-centricity
IoP Layer: Technical
Relevant Legislation: European Accessibility Act, Accessibility Requirements for Products and Services (EU 2019/882); Web Accessibility Directive (EU 2016/2102)
Relevant IE Solution: WCAG 2.0 standard

RC3.7 Implement interoperable service-integration layers

Digital public services should follow a layered architecture separating presentation, process, data, technical components and integration tiers, as defined by the EIF and EIRA models. This ensures modularity, scalability, and alignment across systems. CIO offices and enterprise architects oversee digital public services architecture design and conformance reviews, ensuring consistency between national and EU architectures.

Nature: Mandatory
Stakeholder Roles: Public service providers, Service designers, ICT providers
EIF Principle: 6 – Established standards and common specifications
IoP Layer: Semantic, technical
Relevant Legislation: Interoperable Europe Act (EU 2024/903)
Relevant IE Solution: EIRA

RC3.8 Adopt API-first and data space integration principles

Public-sector data and functionalities should be made available through secure, documented APIs, compatible with EU Data Spaces. Binding for cross-border exchanges, this approach allows interoperability, openness, and innovation. API catalogues, governance rules, and conformance testing ensure reliability.

Nature: Mandatory
Stakeholder Roles: Public service providers, Service designers, ICT providers
EIF Principle: 9 – Data agency / EU data sovereignty
IoP Layer: Semantic, technical
Relevant Legislation: Data Act (EU 2023/2854); Data Governance Act (EU 2022/868)
Relevant IE Solution: --

RC3.9 Guarantee security and privacy across interoperable chains

Security and privacy must be integral to every interoperable service, ensuring trust and compliance with NIS2 and GDPR. CISOs and data-protection officers conduct risk assessments and continuous monitoring, ensuring encryption, trust, and secure access across all nodes.

Nature: Mandatory
Stakeholder Roles: Public service providers, Service designers, ICT providers
EIF Principle: 10 – Trustworthiness
IoP Layer: Technical
Relevant Legislation: NIS2 Directive (EU 2022/2555); GDPR (EU 2016/679)
Relevant IE Solution: --

RC3.10 Ensure multilingual and cultural interoperability via AI

Services should function seamlessly across languages and cultural contexts to ensure inclusiveness and equal participation. This recommendation involves translation APIs, multilingual glossaries, and ontology mappings that maintain semantic equivalence. The eTranslation API integrated into national portals exemplifies multilingual interoperability in action.

Nature: Optional
Stakeholder Roles: Public service providers, Service designers, ICT providers

EIF Principle: 12 – AI for interoperability and interoperability for AI
IoP Layer: Technical, semantic
Relevant Legislation: --
Relevant IE Solution: eTranslation API

RC3.11 Introduce interoperability testbeds and sandboxes

Testbeds and sandboxes enable administrations to validate interoperability and performance before full deployment. Recommended for large or cross-border systems, these controlled environments reduce risks and increase reliability. The CEF Testbed can serve as a model for pre-deployment interoperability testing.

Nature: Optional
Stakeholder Roles: Public service providers, Service designers, ICT providers
EIF Principle: 11 – Assess, improve, deliver
IoP Layer: Technical
Relevant Legislation: AI Act (EU 2024/1689)
Relevant IE Solution: --

RC3.12 Ensure service lifecycle management and continuous improvement

Every service should have a defined lifecycle, from design to decommissioning, with regular updates and quality monitoring. This practice ensures resilience, sustainability, and version control, measured through service-level agreements and dashboards.

Nature: Mandatory
Stakeholder Roles: Public service providers, Service designers, ICT providers
EIF Principle: 11 – Assess, improve, deliver
IoP Layer: All
Relevant Legislation: --
Relevant IE Solution: --

RC3.13 Leverage AI for intelligent service personalisation

AI can tailor services to users' needs, provided it respects transparency, accountability, and interoperability principles. This recommendation requires AI modules with explainability metadata and bias testing, ensuring compliance with the AI Act.

Nature: Optional
Stakeholder Roles: Public service providers, Service designers, ICT providers
EIF Principle: 12 – AI for interoperability and interoperability for AI
IoP Layer: Technical
Relevant Legislation: AI Act (EU 2024/1689)
Relevant IE Solution:

RC3.14 – Implement event-driven interoperability

Adopting event-based architectures enables services to react in real-time across administrative boundaries. Recommended for adaptive systems, this approach employs event schemas and message brokers to automate workflows. Metrics such as latency and reliability demonstrate success.

Nature: Optional
Stakeholder Roles: Public service providers, Service designers, ICT providers
EIF Principle: 5 – Connected and effortless public services
IoP Layer: Technical, semantic
Relevant Legislation: --
Relevant IE Solution: --

RC3.15 – Foster cross-border and cross-sector service federation

Public services should interconnect across borders and sectors to form federated ecosystems. Binding for EU-level services, this approach relies on common protocols and trust registries. The European Digital Identity Wallet represents a concrete example of service federation at scale.

Nature: Optional
Stakeholder Roles: Public service providers, Service designers, ICT providers
EIF Principle: 9 – Data agency / EU data sovereignty
IoP Layer: All

Relevant Legislation: eIDAS (EU 910/2014); European Digital Identity Framework (EU 2024/1184)

Relevant IE Solution: --

RC3.16 – Establish metrics and monitoring for interoperable service performance

Interoperability must be measured through shared indicators and dashboards aligned with the Interoperable Europe Act. Monitoring agencies collect and publish performance data, supporting continuous improvement. The eGovernment Benchmark provides a proven reference model.

Nature: Mandatory

Stakeholder Roles: Public service providers, Service designers, ICT providers

EIF Principle: 11 – Assess, improve, deliver

IoP Layer: All

Relevant Legislation: Interoperable Europe Act (EU 2024/903)

Relevant IE Solution: The eGovernment Benchmark

RC3.17 – Integrate sustainability and green interoperability

Digital public services should minimise environmental impact and contribute to sustainability goals. Recommended under the European Green Deal, this requires energy-efficient infrastructures and carbon monitoring tools. Green ICT practices, such as EU sustainable cloud infrastructures, illustrate this direction.

Nature: Optional

Stakeholder Roles: Public service providers, Service designers, ICT providers

EIF Principle: 8 – In synergy with EU values and legislation

IoP Layer: Technical

Relevant Legislation: EU Green Deal framework

Relevant IE Solution: --

4.4. Developing interoperability solutions

Table 6: Summary of Recommendations for Developing interoperability solutions Scenario

Rec #	Recommendation	Stakeholders	IoP Layers	EIF Principles	Relevant legislation	Relevant IoP Solutions
RC4.1	Develop solutions following the EIF principles and EIRA architecture	ICT providers	Technical	6 – Established standards and common specifications	Interoperable Europe Act (EU) 2024/903	EIRA
RC4.2	Adopt open-source and open-standard approaches	Public service providers; Service designers; ICT providers	All	3 – Efficiency through reuse	Open Data Directive (EU) 2019/1024	Interoperable Europe Portal
RC4.3	Transparent and Open Documentation for Interoperability Components	ICT Providers	Technical	2 – Transparent by design	Data Act (EU) 2023/2854; Data Governance Act (EU) 2022/868	SEMIC Core Vocabularies; CAMSS; API4EU
RC4.4	Ensure modularity and reusability of solutions	Service designers; ICT providers	Technical	3 – Efficiency through reuse	Interoperable Europe Act (EU) 2024/903	
RC4.5	Don't prematurely align to existing specifications	ICT providers; public service providers	Technical	6 – Established standards and common specifications	Interoperable Europe Act (EU) 2024/903	
RC4.6	Implement lifecycle management for interoperability assets	ICT providers; public service providers	Organisational, Technical	11 – Assess, improve, deliver		SEMIC Core Vocabularies
RC4.7	Establish certification and conformance mechanisms	ICT providers; public service providers	Technical, Legal	10 – Trustworthiness		
RC4.8	Provide documentation and knowledge	ICT providers; public service providers	Organisational, Semantic	2 – Transparent by design		API Gateway; Developer Documentation Portal

Rec #	Recommendation	Stakeholders	IoP Layers	EIF Principles	Relevant legislation	Relevant IoP Solutions
	transfer mechanisms					
RC4.9	Integrate solution observability and performance monitoring	ICT providers; public service providers	Organisational, Technical	11 – Assess, improve, deliver	Interoperable Europe Act (EU) 2024/903	OOTS Performance Dashboard; Monitoring Framework
RC4.10	Build a federation of interoperability solution providers	Policy makers; Public service providers; Service designers	Organisational	8 – In synergy with EU values and legislation	Interoperable Europe Act (EU) 2024/903	Interoperable Europe Community of Practice

RC4.1 Develop solutions following the EIF principles and EIRA architecture

All interoperability solutions and relevant infrastructures should conform to EIF principles and EIRA views, ensuring consistency, scalability, and reusability. Binding for EU-funded systems, this requires architecture models, conformance checklists, and review procedures, as seen in the Once-Only Technical System designed under EIRA.

Nature: Mandatory
Stakeholder Roles: ICT providers
EIF Principle: Principle: 6 – Established standards and common specifications
IoP Layer: Technical
Relevant Legislation: Interoperable Europe Act (EU) 2024/903
Relevant IE Solution: EIRA

RC4.2 Adopt open-source and open-standard approaches

Interoperability thrives on openness. Solutions should, whenever possible, adopt open standards and licences that allow reuse and co-development. This requirement strengthens transparency and innovation, exemplified by the Interoperable Europe Portal hosting reusable open components. Developers should, however, avoid using such open components that are not widely adopted and prefer open components that are commonly used across the EU.

Nature: Optional

Stakeholder Roles: Public service providers, Service designers, ICT providers

EIF Principle: 3 – Efficiency through reuse

IoP Layer: All

Relevant Legislation: Open Data Directive (EU) 2019/1024

Relevant IE Solution: Interoperable Europe Portal

RC4.3 Transparent and Open Documentation for Interoperability Components

ICT Providers developing interoperability solutions should produce complete, open, and publicly accessible documentation for all system components (including interfaces, data models, and algorithms) to ensure traceability, reusability, and accountability. Data Providers must maintain well-documented and provenance-traceable datasets aligned with FAIR (Findable, Accessible, Interoperable, and Reusable) principles, enabling others to understand and verify data structures. Public Service Providers procuring or operating interoperability solutions should require transparent documentation and version control from their suppliers, ensuring that components can be independently reviewed and reused. Standardisation Bodies should define and promote common semantic vocabularies, reference data models, and metadata standards that support openness and cross-border interoperability. Transparent governance of interoperability assets should be maintained through open repositories, version control, and peer review mechanisms.

Nature: Mandatory
Stakeholder Roles: ICT Providers
EIF Principle: 2 – Transparent by design
IoP Layer: Technical
Relevant Legislation: Regulation (EU) 2023/2854 (Data Act); Regulation (EU) 2022/868 (Data Governance Act)
Relevant IE Solution: SEMIC Core Vocabularies; CAMSS; API4EU

RC4.4 Ensure modularity and reusability of solutions

Solutions should be modular, interoperable, and designed for reuse across contexts. An organisational process is established of what will constitute a specification and what won't. For example, specifications should be split in the types of specifications as follows:

- **Vocabularies / Taxonomies / Code lists:** Terms to be reused across use cases.
- **Application profiles / schemas:** A use case works in a specific application only when exactly these terms have been provided.
- **Interaction patterns:** A use case only works with a set of interaction patterns.
- **Implementation guides:** The set of application profiles and interaction patterns to be used to achieve interoperability for this specific use case.

Nature: Mandatory
Stakeholder Roles: Service designers, ICT providers
EIF Principle: 3 – Efficiency through reuse
IoP Layer: Technical
Relevant Legislation: Interoperable Europe Act (EU) 2024/903
Relevant IE Solution:

RC4.5 Don't prematurely align to existing specifications

Don't prematurely align to existing specifications if the specification does not exactly fit your use case. Instead, in this case document your own domain model first, and align only when it becomes necessary to do so.

Nature: Optional
Stakeholder Roles: ICT providers, public service providers
EIF Principle: 6 – Established standards and common specifications
IoP Layer: Technical
Relevant Legislation: Interoperable Europe Act (EU) 2024/903
Relevant IE Solution:

RC4.6 Implement lifecycle management for interoperability assets

Sustainable interoperability requires defined version control, maintenance, and deprecation policies. Regular audits and version histories guarantee stability and predictability, as in SEMIC's continuous management of Core Vocabularies.

Nature: Mandatory
Stakeholder Roles: ICT providers, public service providers
EIF Principle: 11 – Assess, improve, deliver (effectiveness & efficiency)
IoP Layer: Organisational, Technical
Relevant Legislation:
Relevant IE Solution: SEMIC Core Vocabularies

RC4.7 Establish certification and conformance mechanisms

Certification processes can help ensure that solutions meet interoperability standards and specifications and can safely interconnect across borders. Interoperability testing and certification, like that under eIDAS trust services, verify compliance and quality assurance.

Nature: Mandatory
Stakeholder Roles: ICT providers, public service providers
EIF Principle: 10 – Trustworthiness ("Security, privacy and trust enable interoperability.")
IoP Layer: Technical, Legal
Relevant Legislation:
Relevant IE Solution:

RC4.8 Provide documentation and knowledge transfer mechanisms

Comprehensive, user-friendly documentation should accompany every solution, ensuring that future developers can maintain and evolve it. Wikis, onboarding guides, and shared repositories support effective knowledge transfer, exemplified by API Gateway documentation on the Interoperable Europe Portal.

Nature: Mandatory
Stakeholder Roles: ICT providers, public service providers
EIF Principle: 2 – Transparent by design ("You can't trust what you can't understand.")
IoP Layer: Organisational, Semantic
Relevant Legislation:
Relevant IE Solution: API Gateway / Developer Documentation Portal (Interoperable Europe)

RC4.9 Integrate solution observability and performance monitoring

Every operational component should include built-in metrics for reliability, performance, and interoperability. Monitoring dashboards like the OOTS performance system provide real-time visibility and early issue detection.

Nature: Mandatory
Stakeholder Roles: ICT providers, public service providers
EIF Principle: 11 – Assess, improve, deliver (effectiveness & efficiency)
IoP Layer: Organisational, Technical
Relevant Legislation: Interoperable Europe Act (EU) 2024/903
Relevant IE Solution: OOTS Performance Dashboard / Monitoring Framework

RC4.10 Build a federation of interoperability solution providers

Europe should cultivate a trusted network of public and private entities that co-develop and maintain interoperable assets. This federated approach, promoted by the Interoperable Europe Community of Practice, ensures continuous innovation and shared stewardship.

Nature: Mandatory
Stakeholder Roles: Policy makers, Public service providers, Service designers
EIF Principle: 8 – In synergy with EU values and legislation
IoP Layer: Organisational
Relevant Legislation: Interoperable Europe Act (EU) 2024/903
Relevant IE Solution: Interoperable Europe Community of Practice

4.5. Interoperability Governance

Table 7: Summary of Recommendations for Interoperability Governance

Rec#	Recommendation	Main stakeholder roles	IoP Layers	EIF Principles	Relevant legislation	Relevant IoP Solutions
RC5.1	Ensure Multi-Level Interoperability Governance and Alignment between NIFs and the EIF	Legislators, policy makers	All	1 – Subsidiarity and proportionality	Interoperable Europe Act	Interoperable Europe Board (governance mechanism), NIFO Observatory (EU repository of NIFs)
RC5.2	Assign clear interoperability leadership and accountability	Policy makers		10 – Trustworthiness		
RC5.3	Establish Interoperability Observatories and Dashboards with Assessment and Compliance Mechanisms	Legislators, Policy makers, ICT providers, Public service providers	All	11 – Assess, improve, deliver (effectiveness & efficiency)	Interoperable Europe Act	Interoperable Europe Observatory, EIF4SCC Self-Assessment Tool
RC5.4	Integrate interoperability into funding and procurement criteria	Legislators, Policy makers		7 – Readiness for interoperability as a conditionality	Interoperable Europe Act	
RC5.5	Build an Interoperability Competence Network	Legislators, Policy makers, ICT providers, Public service	All	8 – In synergy with EU values and legislation	Interoperable Europe Act	Interoperable Europe Academy

Rec#	Recommendation	Main stakeholder roles	IoP Layers	EIF Principles	Relevant legislation	Relevant IoP Solutions
		providers, Standardisation bodies, Service Designers, Data providers				
RC5.6	Ensure stakeholder engagement and transparency	Policy makers, Public service providers, Public service consumers, Standardisation bodies	All	2 – Transparent by design, 8 – In synergy with EU values and legislation, 11 – Assess, improve, deliver (effectiveness & efficiency)	Interoperable Europe Act, AI Act, Data Act	Interoperable Europe Community Forum; NIFO Observatory; NIFO Benchmark Framework; Interoperable Europe Portal; EIF Periodic Revision Process; EU Survey; AI Office EU Framework; Joinup Platform
RC5.7	Link interoperability governance with cybersecurity and data governance	Legislators, Policy makers, Public service providers	All	10 – Trustworthiness	NIS2 Directive (Data Governance Act	
RC5.8	Promote interoperability innovation and experimentation	Legislators, ICT providers, Public service providers	All	13 – AI for interoperability and interoperability for AI	AI Act	GovTech Labs; Interoperable Europe Innovation Boards
RC5.9	Establish funding mechanisms for long-term sustainability	Policy makers	Organisational	7 – Readiness for interoperability as a conditionality	Interoperable Europe Act Digital Europe Program	

RC5.1 Ensure Multi-Level Interoperability Governance and Alignment between NIFs and the EIF

A coherent governance model must link EU, national, and local levels under common roles and processes. The Interoperable Europe Board exemplifies this multi-level coordination, aligning national strategies with EU principles. Every Member State should operate a living NIF harmonised with the EIF. Regular assessments and updates ensure that national frameworks evolve in sync with EU interoperability directions, as exemplified by the Italian ModI and Danish NIF.

Nature: Mandatory
Stakeholder Roles: All
EIF Principle: 1 – Subsidiarity and proportionality
IoP Layer: All
Relevant Legislation: Interoperable Europe Act (EU) 2024/903
Relevant IE Solution: Interoperable Europe Board (governance mechanism), NIFO Observatory (EU repository of NIFs)

RC5.2 Assign clear interoperability leadership and accountability

Each administration should appoint accountable interoperability leaders, typically CIOs or designated coordinators, empowered to enforce EIF principles. Transparency in roles and mandates ensures effective decision-making and oversight.

Nature: Mandatory
Stakeholder Roles: Legislators, Policymakers
EIF Principle: 10 – Trustworthiness (security, privacy and accountability)
IoP Layer: Legal, organisational
Relevant Legislation: --
Relevant IE Solution: --

RC5.3 Establish Interoperability Observatories and Dashboards with Assessment and Compliance Mechanisms

Monitoring through interoperability observatories provides quantitative insight into progress and maturity. Annual reports, indicators, and dashboards, like those of the Interoperable Europe Observatory, guide continuous improvement. Self-assessment and audit tools should measure compliance with EIF standards and highlight areas for correction. The EIF4SCC self-assessment tool provides a practical example of such governance mechanisms in action.

Nature: Mandatory
Stakeholder Roles: Public service providers, Service designers, ICT providers
EIF Principle: 11 – Assess, improve, deliver (effectiveness & efficiency)
IoP Layer: All
Relevant Legislation: Interoperable Europe Act (EU) 2024/903

Relevant IE Solution: Interoperable Europe Observatory, EIF4SCC Self-Assessment Tool

RC5.4 Integrate interoperability into funding and procurement criteria

All EU and national funding instruments should include EIF compliance as an eligibility or evaluation criterion. Programmes such as Digital Europe and CEF Digital already embed this requirement in procurement templates.

Nature: Optional
Stakeholder Roles: Policymakers, Public service providers
EIF Principle: 7 – Readiness for interoperability as a conditionality
IoP Layer: Legal, organisational, technical
Relevant Legislation: Interoperable Europe Act (EU) 2024/903
Relevant IE Solution:--

RC5.4 Build an Interoperability Competence Network

Developing a skilled community of practitioners is key to long-term success. The Interoperable Europe Academy and national training programmes ensure that officials and experts have the competencies to apply EIF principles in practice.

Nature: Mandatory
Stakeholder Roles: Policymakers, Public service providers
EIF Principle: 8 – In synergy with EU values and legislation
IoP Layer: All
Relevant Legislation: Interoperable Europe Act (EU) 2024/903
Relevant IE Solution: Interoperable Europe Academy

RC5.6 Ensure stakeholder engagement and transparency

Governance must be participatory, transparent and accountable. Governance structures, decision criteria, and evaluation procedures should be publicly documented and accessible, allowing external review and stakeholder input. Regular consultations through digital platforms like the Interoperable Europe Community Forum ensure that industry, academia, and citizens contribute to decision-making. Public Service Providers must maintain open registries of interoperability assets, data models, and algorithms used in public administration, together with clear accountability lines for their management. Standardisation Bodies should coordinate transparent and inclusive consultation

processes for developing and maintaining interoperability standards, ensuring openness and traceability in revisions and updates. Interoperability governance must evolve dynamically, integrating lessons learned and new technologies. Annual review cycles and stakeholder input ensure relevance and agility, as done in the EIF periodic revision process.

Nature: Mandatory

Stakeholder Roles: Policymakers, Public service providers

EIF Principle: 2 – Transparent by design, 8 – In synergy with EU values and legislation, 11 – Assess, improve, deliver (effectiveness & efficiency)

IoP Layer: Legal, organisational

Relevant Legislation: Interoperable Europe Act (EU) 2024/903, Regulation (EU) 2024/1689 (AI Act); Regulation (EU) 2023/2854 (Data Act)

Relevant IE Solution: Interoperable Europe Community Forum, NIFO Observatory; NIFO Benchmark Framework; Interoperable Europe Portal; EIF Periodic Revision Process; AI Office EU Framework; Joinup Platform

RC5.7 Link interoperability governance with cybersecurity and data governance

Strong alignment with related governance areas, such as: cybersecurity, privacy, and data policy, ensures coherence. Coordinated structures prevent overlap and enable integrated risk management, exemplified by synergy between NIS2, DGA, and EIF.

Nature: Optional

Stakeholder Roles: Public service providers, Service designers, ICT providers

EIF Principle: 10 – Trustworthiness

IoP Layer: Technical

Relevant Legislation: NIS2 Directive (EU) 2022/2555; Data Governance Act (EU) 2022/868

Relevant IE Solution: --

RC5.8 Promote interoperability innovation and experimentation

Governance should foster experimentation through sandboxes and pilot environments that test new approaches before formal adoption. GovTech Labs and innovation boards offer successful models for such experimentation.

Nature: Optional

Stakeholder Roles: Policymakers, Public service providers

EIF Principle: 12 – AI for interoperability and interoperability for AI

IoP Layer: All
Relevant Legislation: AI Act (EU) 2024/1689
Relevant IE Solution: GovTech Labs; Interoperable Europe Innovation Boards

RC5.9 Establish funding mechanisms for long-term sustainability

Stable and predictable funding is the cornerstone of sustainable interoperability governance. Multi-annual frameworks and co-financing arrangements, like those of the Digital Europe Programme, guarantee the continuity of shared assets and institutions.

Nature: Optional
Stakeholder Roles: Policymakers, Public service providers
EIF Principle: 7 – Readiness for interoperability as a conditionality
IoP Layer: Legal, organisation, governance
Relevant Legislation: Interoperable Europe Act (EU) 2024/903; Digital Europe Programme
Relevant IE Solution: --

5. Application Guidance: The EIF Cookbook

The EIF is not only a set of principles and recommendations; it is a practical instrument meant to be applied in daily administrative and policy work. To help administrations move from theory to action, the "EIF Cookbook" provides a structured, hands-on approach for the application of the EIF. Like a real cookbook, it offers guidance to all EIF stakeholders and practitioners, in their quest to translate recommendations into concrete measures, building digital services that are interoperable, inclusive, and sustainable.

EIF Cookbook

Develop or Align NIF
Create a national framework consistent with EIF

Monitor and Evaluate Progress
Assess interoperability maturity and impact

Conduct Training
Build capacity among professionals

Leverage Interoperable Solutions
Reuse existing assets for efficiency

Build Community
Foster collaboration and knowledge exchange

Apply EIF Scenarios
Embed EIF principles in public sector lifecycle

Use Testing Environments
Validate interoperability solutions safely

Align with Legislation
Ensure coherence with EU legal landscape

Integrate AI
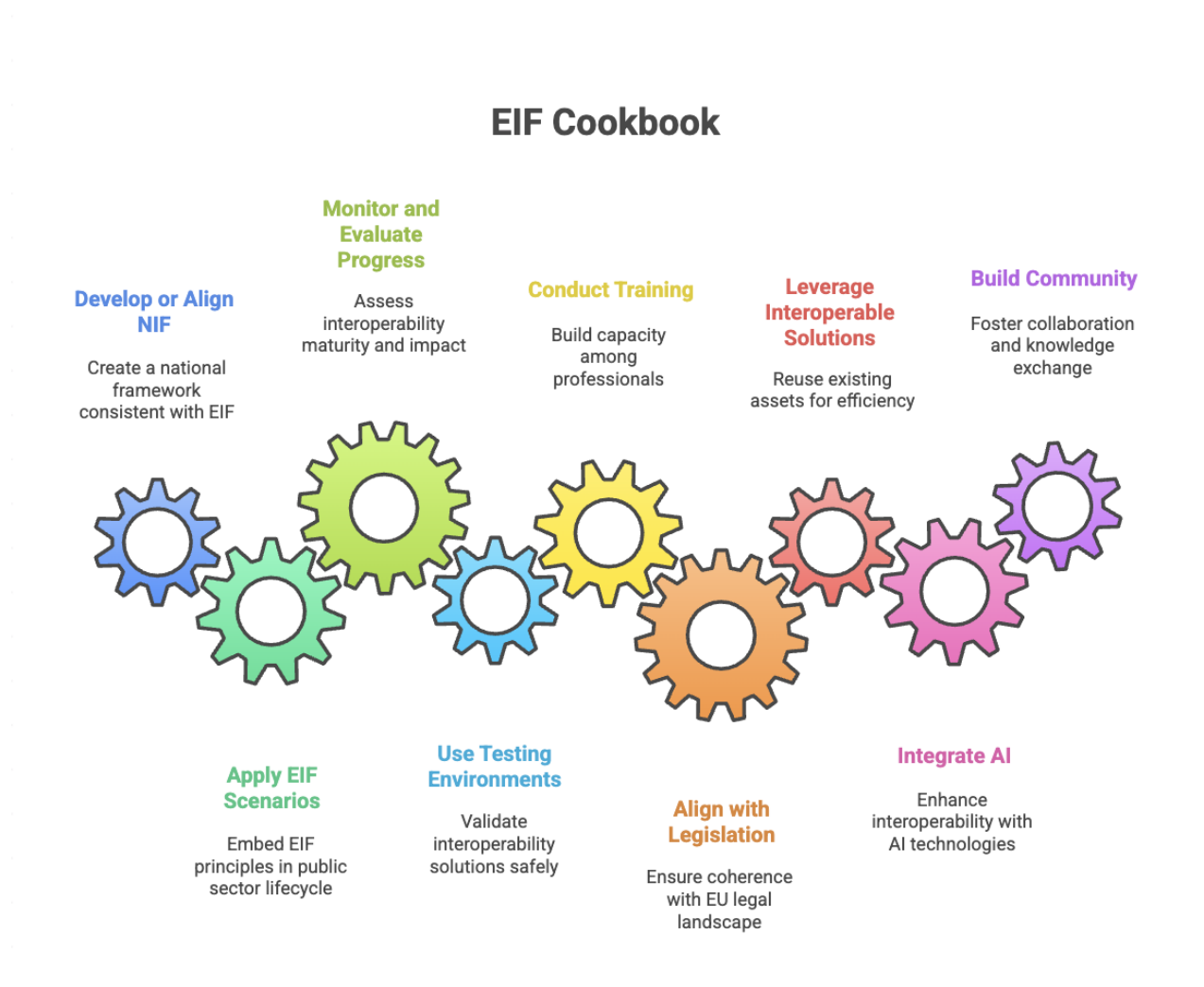Enhance interoperability with AI technologies

Figure 4: EIF Cookbook

5.1 Develop or Align Your National Interoperability Framework (NIF)

Since the EIF is an EU-wide framework, including universal principles and recommendations for interoperability in digital public services, its instantiation in member states' specific strategies or situations is needed. So, each Member State is encouraged to develop or update its National Interoperability Framework (NIF) so that it reflects the EIF's structure, principles, and recommendations adapted in its own needs. This process involves analysing existing national digital strategies, enterprise architectures, and legal frameworks, and mapping them against the EIF to identify overlaps and gaps. Where differences exist, governments should plan for convergence through coordinated actions, new governance mechanisms, and updated monitoring indicators.

Periodic self-assessments, using established interoperability maturity models or dashboards, can support this alignment process and track national progress over time.

The following key actions and steps are envisaged:

- Establish or revise a national framework consistent with EIF principles and recommendations. Try to reference the EIF principles and recommendations, adding extra specifications, mention to existing infrastructures, or proposed standards where required.
- Map existing strategies, laws, and architectures against EIF recommendations to identify gaps.
- Define national governance and monitoring mechanisms.
- Ensure periodic updates reflecting new EU legislation and technological trends.
- Use interoperability maturity tools and self-assessments to measure progress and alignment.
- Any deviation from EIF principles or recommendations should be properly justified and documented.

The above guidelines also govern the development of sector-specific interoperability frameworks (e.g. related to health, education, or financial services) or other organisation-specific interoperability frameworks (e.g. interoperability frameworks for local administration organisations of a member state, or a European Commission agency).

5.2 Apply the EIF in Practice, through its Application Scenarios

Once national frameworks are aligned, or even when there is no NIF in place, the EIF proposes four main application scenarios that show how its principles and recommendations can be embedded across the public sector lifecycle.

When drafting and evaluating legislation, policymakers should ensure that new laws enable data sharing, reuse, and interoperability by design. In designing public policies, interoperability must be considered from the early stages of problem definition and stakeholder consultation. Then, in delivering public services, administrations should apply the EIF's conceptual dimensions (legal, organisational, semantic, and technical) to guarantee seamless user experiences across borders and sectors. Finally, in developing interoperability solutions, teams can make use of the Interoperable Europe Solutions, to adopt common specifications, APIs, and reference architectures that ensure consistency and efficiency.

The following key actions are proposed:

- Analyse the EIF principles and recommendations, deciding on the minimum level of conformance.
- Use dashboards, testbeds, and evidence-based indicators to monitor impact.
- Report findings through Interoperable Europe Portal and the NIFO observatory.
- Share lessons learned and best practices to promote mutual learning and continuous improvement.

5.3 Monitor, Evaluate, and Share Interoperability Progress

Monitoring and evaluation ensure that interoperability policies produce measurable results. Administrations are encouraged to establish mechanisms for assessing maturity, adoption, and impact both at organisational and national levels. Dashboards, testbeds, and evidence-based indicators can support this process, showing how digital services evolve toward higher levels of interoperability. Reporting and benchmarking through the Interoperable Europe platform allow Member States to exchange knowledge, showcase best practices, and identify areas for improvement. By sharing results openly, administrations contribute to a collective European learning process, reinforcing transparency, accountability, and mutual trust.

The following key activities are proposed:

- Set up mechanisms to assess maturity and measure adoption at organisational and national level.
- Use dashboards, testbeds, and evidence-based indicators to monitor impact.
- Report findings towards the Interoperable Europe community.
- Share lessons learned and best practices to promote mutual learning and continuous improvement.

5.4 Using Testing and Sandboxing Environments

Testing and sandboxing environments are key tools for risk-free experimentation with interoperability solutions. They allow teams to validate data exchange mechanisms, authentication processes, and semantic mappings before deploying them in production environments. Such controlled settings encourage innovation while ensuring compliance with the EIF and relevant EU legislation such as the AI Act, Data Governance Act, and Cybersecurity Act. Testbeds like the CEF Interoperability Testbed and national equivalents can serve as reference infrastructures for joint experimentation, cross-border testing, and quality assurance. Through these environments, administrations can accelerate innovation while maintaining reliability and trustworthiness.

Organise your activities along the following lines:

- Use testbeds and sandboxes to validate interoperability solutions safely before full deployment.
- Experiment with data exchange, authentication, and semantic mapping services.
- Evaluate compliance with EIF principles and relevant legislation (AI Act, Data Act, etc.).
- Foster innovation while managing risk, ensuring scalability and conformance to EU standards.

5.5 Training and Capacity Building on the EIF

Successful EIF implementation requires skilled professionals and informed decision-makers. Capacity building should therefore be an integral component of every national or organisational action plan. Training programmes can be developed for policymakers, enterprise architects, project managers, and technical experts, covering both theoretical understanding and hands-on practice. EIF-based modules can be integrated into national public administration academies, universities, and professional schools. E-learning resources, peer exchanges, and micro-credential systems can help build a sustainable community of interoperability practitioners who share a common vocabulary and mindset.

Continuous learning ensures that interoperability evolves alongside technological and policy innovation.

The following key actions are proposed:

- Develop structured training for policymakers, architects, and IT professionals.
- Integrate EIF modules into national academies and public-sector curricula.
- Get ideas, courses, educational material, and assessment tests from the Interoperability Academy.
- Offer online courses, peer exchanges, and micro-credentials on interoperability.
- Build a professional community able to maintain and evolve interoperable services sustainably.

5.6 Addressing Related Legislation

EIF application does not occur in isolation - it must align with the broader EU legal landscape governing digital governance and data use. Key legislative instruments include the Interoperable Europe Act, the Data Act, the EU AI Act, the eIDAS 2 Regulation, the Open Data Directive, and others. Creating and maintaining a living reference list of these legal acts helps ensure coherence between regulatory obligations and interoperability practices. This alignment requires collaboration between legal experts, policy designers, and IT professionals, ensuring that interoperability solutions remain lawful, ethical, and technically sound across jurisdictions.

The European Commission maintains an updated list of relevant to the EIF legislation at the Interoperable Europe Portal (*Link to be provided*).

5.7 Leveraging Interoperable Europe Solutions

A cornerstone of EIF implementation is the reuse of existing assets through the Interoperable Europe Solutions Catalogue. Administrations should systematically explore, select, and adapt the available solutions - such as eDelivery, eID, the Once-Only Technical System, and the EIRA reference architecture.

A simple workflow can be followed: *discover - select - adapt - test - deploy - share back*. This cycle promotes efficiency, avoids duplication, and reinforces European digital sovereignty through collective ownership of public-sector technology. By contributing improvements

and sharing local adaptations, each administration strengthens the common foundation of interoperable public services in Europe.

European Commission maintains an updated list of Interoperable Europe Solutions at the Interoperable Europe Portal (*Link to be provided*)

5.8 Using Artificial Intelligence for Achieving Interoperability

Artificial Intelligence is becoming an enabler of interoperability across data, processes, and organisations. AI systems can automate data classification, semantic matching, and multilingual translation—reducing manual workload and improving consistency. Process-oriented AI can support automated compliance checks, policy alignment, and early detection of interoperability bottlenecks. Predictive and generative AI tools can further assist in creating harmonised documentation, translating legal texts, and facilitating communication with citizens.

When used responsibly and transparently - according to the principles of the EU AI Act – artificial intelligence becomes a catalyst for achieving interoperable, smart, and adaptive public services that align with the EIF vision.

Proposed actions to achieve interoperability through the use of AI, at legal, organisational, semantic, technical and interoperability governance layers, as well as on Interoperability Governance are listed in ANNEX 3.

5.9 Building a Community of Practice

Interoperability is a shared European endeavour that depends on collaboration and trust. Building a vibrant community of practice around the EIF and the various NIFs ensures that experience, tools, and knowledge are continually exchanged.

Through the Interoperable Europe Community, stakeholders can co-create new assets, participate in thematic working groups, and support each other's implementation efforts. Such a community not only accelerates EIF adoption but also guarantees that the framework remains a living, evolving instrument—one that reflects the collective intelligence and creativity of Europe's public sector professionals.

Key actions towards making interoperability governance a more collaborative task are the following:

- Foster an active community under the Interoperable Europe initiative.
- Encourage exchange of experiences, case studies, and reusable solutions.
- Support cross-border networks and thematic working groups.
- Keep NIF a living, evolving framework co-created by its practitioners.

ANNEXES

ANNEX 1. Abbreviations

Abbreviation	Term
AI	Artificial Intelligence
API	Application Programming Interface
CEF	Connecting Europe Facility
CIO	Chief Information Officer
DCAT-AP	Data Catalog Vocabulary – Application Profile
EIRA	European Interoperability Reference Architecture
EIF	European Interoperability Framework
eIDAS	Electronic Identification, Authentication and Trust Services
EUPL	European Union Public Licence
GDPR	General Data Protection Regulation
HL7 - FHIR	Health Level 7 – Fast Healthcare Interoperability Resources
ICT	Information and Communication Technology
IEA	Interoperable Europe Act
IE	Interoperable Europe
ISO	International Organization for Standardization
LLM	Large Language Model
MIT	Massachusetts Institute of Technology (Licence)
NLP	Natural Language Processing
NIF	National Interoperability Framework
NIS2	Network and Information Security Directive (version 2)
OECD	Organisation for Economic Co-operation and Development
OOTS	Once-Only Technical System
PSD2	Payment Services Directive 2
RC	Recommendation Code
SIF	Specialised Interoperability Framework
SEMIC	Semantic Interoperability Community
UN	United Nations

ANNEX 2. Relevant Legislation Catalogue

This list of relevant legislation elements **should be outside the text of the EIF** and maintained in a proper internet page. Only the link to this page should be included in the EIF.

Num	Legal Element	Link
01	Interoperable Europe Act (EU) 2024/903	
02	Single Digital Gateway Regulation (EU) 2018/1724	
03	e-IDAS (EU) 910/2014	
04	European Digital Identify Framework (EU) 2024/1184	
05	Accessibility Requirements for Products and Services (EU) 2019/882	
06	Open Data Directive	
07	NIS2 Directive (EU) 2022/2555	
08	General Data Protection Regulation (EU) 2016/679	
09	AI Act (EU) 2024/1689	
10	Cyber Resilience Act (EU) 2024/2847	
11	Digital Service Act (EU) 2022/2065	
12	Data Act (EU) 2023/2854	

ANNEX 3. AI for Interoperability: Indicative actions

Below some key AI-enabled actions across the Interoperability Layers are listed.

A3.1 Legal Interoperability

Using AI to interpret, align, and ensure compliance of legal and regulatory frameworks across jurisdictions.

- Automatically classify and tag legislation based on interoperability relevance
- Automate impact assessments on interoperability when new legislation is proposed.
- Use Natural Language Processing (NLP) and properly trained large language models (LLMs) to extract obligations and rights from legal texts, for automated mapping.
- Employ AI models for legal harmonisation, comparing national laws with EU directives to identify inconsistencies.
- Implement AI-driven conformity checking between legal provisions and service implementation rules.
- Deploy chatbot / agent legal assistants for interpreting EU digital legislation in plain language for public sector employees.
- Use semantic AI models to align legal terminologies and definitions.
- Develop AI-based citation analysis to track dependencies and conflicts between regulations.
- Train large language models (LLMs) on public-sector law to generate cross-border compliance summaries.

A3.2 Organisational Interoperability

Using AI to improve cooperation, coordination, and alignment among institutions.

- Analyse organisational structures using AI-based network mapping to detect collaboration gaps.
- Apply machine learning to identify redundant processes or overlapping mandates across agencies.
- Use predictive analytics to anticipate interoperability bottlenecks in multi-agency workflows.
- Use AI chatbots as digital assistants for cross-department coordination.
- Analyse communication data to measure collaboration intensity and sentiment between agencies.

- Generate AI-based process alignment recommendations for harmonising organisational procedures.
- Apply AI–driven workflow mining to discover and optimise interoperability-relevant interactions.

A3.3 Semantic Interoperability

Using AI to align data, vocabularies, and meanings across domains and languages.

- Train AI models to map equivalent concepts between heterogeneous data schemas.
- Use semantic embedding models to detect synonymy and hierarchy in taxonomies and ontologies.
- Apply AI for multilingual translation of metadata and controlled vocabularies.
- Generate semantic interoperability mappings automatically between national datasets.
- Use knowledge graphs and AI reasoning to infer missing relationships between datasets.
- Deploy AI agents that validate semantic consistency during data exchange.
- Apply LLMs for data annotation and metadata enrichment in open data portals.
- Automate semantic version tracking, detecting changes in data meaning over time.
- Use AI-driven similarity detection to recommend dataset integration opportunities.
- Build cross-lingual AI models that align terminology from different EU languages in real time.

A3.4 Technical Interoperability

Using AI to enhance infrastructure compatibility, integration, and service reliability.

- Implement AI-based API discovery and matching to facilitate integration between systems.
- Use machine learning to detect interface incompatibilities or data flow errors.
- Apply AI-driven orchestration for automated service composition and workflow adaptation.
- Employ AI-powered testing tools to simulate interoperability scenarios in sandbox environments.
- Use predictive maintenance models for infrastructure supporting interoperability (e.g. gateways, APIs).
- Deploy AI-enhanced cybersecurity monitoring to identify anomalies in cross-border data exchange.
- Create intelligent middleware that adapts automatically to technical standards changes.

- Use AI auto-documentation tools to generate technical specifications and API documentation.
- Apply deep learning for format recognition and conversion of legacy datasets.
- Use reinforcement learning to optimise system interoperability performance parameters.

A3.5 Governance of Interoperability

Using AI to support strategic coordination, compliance, and continuous improvement across governance layers.

- Employ AI-driven dashboards for real-time monitoring of interoperability maturity across Europe.
- Use AI analytics to evaluate policy outcomes and interoperability progress indicators.
- Apply LLMs to draft interoperability policies and frameworks aligned with EIF principles.
- Implement AI-based risk assessment models for interoperability governance and digital sovereignty.
- Use AI to simulate governance scenarios, predicting the impact of policy decisions.
- Automate collection and synthesis of stakeholder feedback from community consultations.
- Apply AI models to detect non-conformance with EIF recommendations across projects.
- Use generative AI to produce accessible reports, summaries, and dashboards for policymakers.
- Build AI-based recommender systems for selecting suitable interoperability solutions or standards.
- Employ ethical AI assistants to support transparent, explainable governance and accountability.

ANNEX 4: References

Annex 4 provides the full list of references and sources cited in the text.