EUROPEAN
COMMISSION

Brussels, 23.3.2017
COM(2017) 134 final

ANNEX 2

ANNEX

to the
COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

European Interoperability Framework - Implementation Strategy

{SWD(2017) 112 final}
{SWD(2017) 113 final}

Contents

TABLE OF FIGURES

1 INTRODUCTION

As stipulated in the Treaties of the European Union (EU), the EU's internal market guarantees four 'freedoms' - the free movement of goods, capital, services and people between the 28 Member States. These freedoms are assured by common policies supported by interconnected, interoperable networks and systems. People are free to work and relocate and businesses are free to trade and operate in all EU Member States. In doing so, they inevitably have to interact electronically with Member State public administrations.

To make these interactions efficient, effective, timely and of high quality, and to help cut red-tape and reduce the cost and effort involved, Member States are modernising their public administrations by introducing digital public services. However, in doing so, they risk creating isolated digital environments and consequently electronic barriers that may prevent public administrations from connecting with each other, and citizens and businesses from identifying and using available digital public services in countries other than their own. For this reason, efforts to digitise the public sector should be well coordinated at European and national levels to avoid digital fragmentation of services and data, and help the EU's digital single market to work smoothly.

At the same time, the challenges facing the Union require common policy responses from the Member States and the Commission, through EU legislation that requires interaction across borders and policy sectors. This also involves setting up and running interoperable systems. Such systems, as set out in the digital single market strategy,[1] are intended to ensure effective communication between digital components such as devices, networks and data repositories. They also provide more efficient connections across borders, between communities and between public services and authorities.

The EIF gives guidance, through a set of recommendations, to public administrations on how to improve governance of their interoperability activities, establish cross-organisational relationships, streamline processes supporting end-to-end digital services, and ensure that existing and new legislation do not compromise interoperability efforts.

1.1 Definitions

1.1.1 Interoperability

For the purpose of the EIF, ***interoperability*** is the ability of organisations[2] to interact towards mutually beneficial goals, involving the sharing of information and knowledge between these

[1] COM(2015) 192 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Single Market Strategy for Europe, Brussels, 06.05.2015.

[2] 'Organisations' here means public administration units or any entity acting on their behalf, or EU institutions or bodies.

organisations, through the business processes they support, by means of the exchange of data between their ICT systems.

1.1.2 European public service

A ***European public service*** comprises any public sector service exposed to a cross-border dimension and supplied by public administrations, either to one another or to businesses and citizens in the Union.

1.1.3 European interoperability framework

The ***European interoperability framework*** is a commonly agreed approach to the delivery of European public services in an interoperable manner. It defines basic interoperability guidelines in the form of common principles, models and recommendations.

1.2 The EIF's purpose and legal framework

The purpose of the EIF is to:

- inspire European public administrations in their efforts to design and deliver seamless European public services to other public administrations, citizens and businesses which are to the degree possible, digital-by-default (i.e. providing services and data preferably via digital channels), cross-border-by-default (i.e. accessible for all citizens in the EU) and open-by-default (i.e. enabling reuse, participation/access and transparency);

- provide guidance to public administrations on the design and update of national interoperability frameworks (NIFs), or national policies, strategies and guidelines promoting interoperability;

- contribute to the establishment of the digital single market by fostering cross-border and cross-sectoral interoperability for the delivery of European public services.

The lack of interoperability is a major obstacle to progress on the digital single market. Using the EIF to steer European interoperability initiatives contributes to a coherent European interoperable environment, and facilitates the delivery of services that work together, within and across organisations or domains.

The EIF is principally promoted and maintained by the ISA² programme[3] in close cooperation between the Member States and the Commission in the spirit of Articles 26, 170 and 171 of the Treaty on the Functioning of the European Union[4] calling for the establishment of

[3] Established by Decision (EU) 2015/2240 of the European Parliament and of the Council of 25 November 2015.
[4] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN.

interoperable trans-European networks that will enable citizens to derive full benefit from a European internal market.

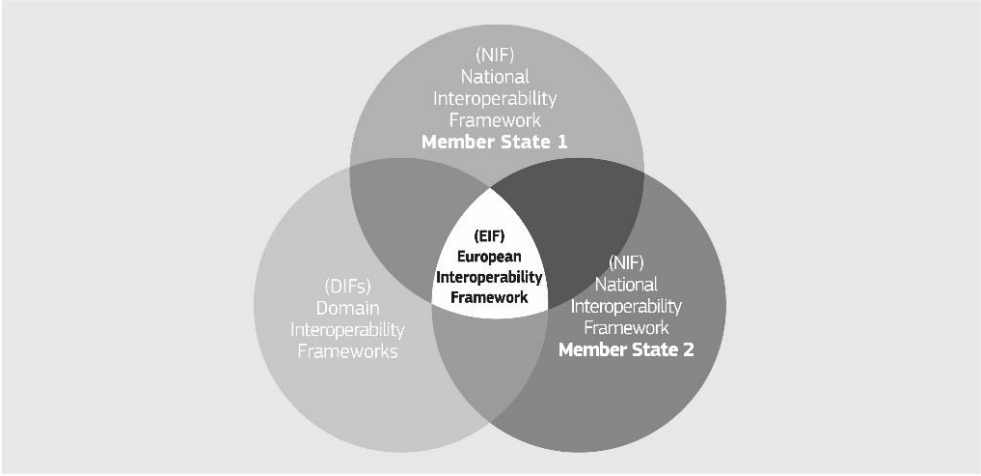
1.3 Scope, readership and usage of the EIF

The EIF is meant to be a **generic framework** applicable to all public administrations in the EU. It lays out the basic conditions for achieving interoperability, acting as the common denominator for relevant initiatives at all levels including European, national, regional and local, embracing public administrations, citizens and businesses. This document is addressed to all those involved in defining, designing, developing and delivering European public services.

As Member States have different administrative and political systems, national specificities have to be taken into account when transposing the EIF into the national context. EU and national policies (e.g. NIFs) are expected to build upon the EIF, by adding new or fine-tuning existing elements. In a similar way, domain-specific interoperability frameworks (DIFs)[5] should remain compatible with, and where necessary extend, the scope of the EIF to capture the specific interoperability requirements of the domain in question. This means that some of the EIF elements can be directly copied into a NIF or DIF, while others might need to be contextualised and further tailored to cover the particular needs.

The relationship among EIF, NIFs and DIFs is described in figure 1. The EIF provides a common core of interoperability elements to European NIFs and DIFs. Compliance with the EIF guarantees that NIFs and DIFs are developed in a coordinated and aligned way while providing the necessary flexibility to address specific requirements coming from national or domain-specific requirements.

Figure 1: Relationship between EIF, NIFs and DIFs



[5] For example Directive 2007/2/EC establishing an Infrastructure for Spatial Information in the European Community (INSPIRE), and the relevant implementing regulations and guidelines.

In general, the EIF provides value in two directions:

- **bottom-up:** when a NIF aligned with the EIF is used for the implementation of public services at all levels of national administrations, it creates the interoperability conditions for extending the scope of these services across borders;
- **top-down:** when the EIF is considered in EU legislation and policy domains, either through ad hoc references or more structurally using DIFs, it increases the interoperability potential of the follow-up national actions resulting from transposition.

In both cases, the end result is the development of a European public services ecosystem in which owners and designers of systems and public services become aware of interoperability requirements, public administrations are ready to collaborate with each other and with businesses and citizens, and information flows seamlessly across borders to support a digital single market in Europe.

1.3.1 Interoperability areas

The EIF's scope covers three types of interactions:

- A2A (administration to administration), which refers to interactions between public administrations (e.g. Member State or EU Institutions);
- A2B (administration to business), which refers to interactions between public administrations (in a Member State or an EU Institution) and businesses;
- A2C (administration to citizen), which refers to interactions between public administrations (in a Member State or an EU institution) and citizens.

1.3.2 Content and structure

The EIF content and structure is presented below:

- Chapter 2 presents a set of **principles** intended to establish general behaviours on interoperability;
- Chapter 3 presents a layered **interoperability model** which organises in layers the different interoperability aspects to be addressed when designing European public services;
- Chapter 4 outlines a conceptual **model for interoperable public services**. The model is aligned with the interoperability principles and promotes the idea of 'interoperability by design' as a standard approach for the design and operation of European public services;
- Chapter 5 concludes the document by providing an overview and **tying together the major elements of the EIF**;

- A set of **47 recommendations,** as actionable items to be implemented by public administrations, is discussed across the different chapters.

2 UNDERLYING PRINCIPLES OF EUROPEAN PUBLIC SERVICES

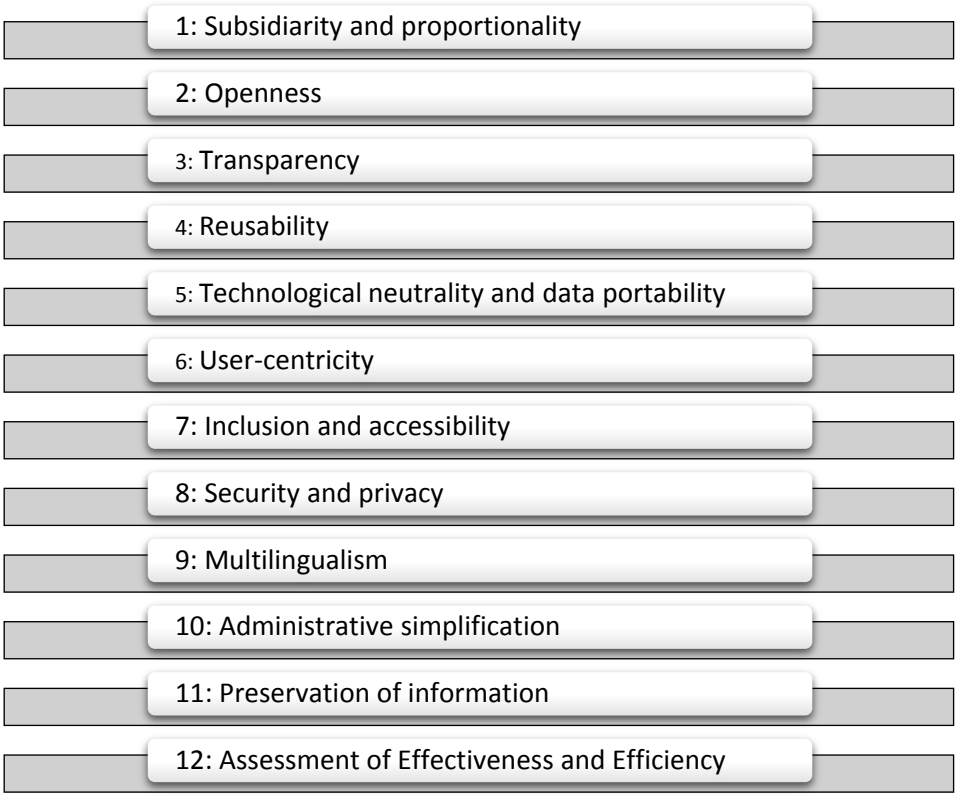
2.1 Introduction

The ***interoperability principles*** are fundamental behavioural aspects to drive interoperability actions. This chapter sets out general interoperability principles which are relevant to the process of establishing interoperable European public services. They describe the context in which European public services are designed and implemented.

The twelve underlying principles[6] of the EIF are grouped into four categories:

1. Principle setting the context for EU actions on interoperability (No 1);
2. Core interoperability principles (Nos 2 to 5);
3. Principles related to generic user needs and expectations (Nos 6 to 9);
4. Foundation principles for cooperation among public administrations (Nos 10 to 12).

Figure 2: Interoperability principles



[6] The principles remain practically the same as in the previous EIF. Their grouping and the exact scope of each recommendation have been updated to reflect recent policy and technical development.

2.2 Underlying principle 1: subsidiarity and proportionality

The **subsidiarity** principle requires EU decisions to be taken as closely as possible to the citizen. In other words, the EU does not take action unless this is more effective than the same action taken at national level. The **proportionality** principle limits EU actions to what is necessary to achieve the objectives of the Treaties.

Concerning interoperability, a European framework is justified to overcome differences in policies that result in heterogeneity and lack of interoperability and that put at risk the digital single market.

The EIF is envisaged as the **'common denominator'** of interoperability policies in Member States. Member States should enjoy sufficient freedom to develop their NIFs with respect to EIF recommendations. NIFs are expected to be tailored and extended in such a way that national specificities are properly addressed.

Recommendation 1:

Ensure that national interoperability frameworks and interoperability strategies are aligned with the EIF and, if needed, tailor and extend them to address the national context and needs.

2.3 Underlying principle 2: openness

In the context of interoperable public services, the concept of **openness** mainly relates to data, specifications and software.

Open government data (here simply referred **'open data'**) refers to the idea that all public data should be freely available for use and reuse by others, unless restrictions apply e.g. for protection of personal data, confidentiality, or intellectual property rights. Public administrations collect and generate huge amounts of data. The Directive on the reuse of public sector information (PSI)[7] encourages Member States to make public information available for access and reuse as open data. The INSPIRE Directive[8] requires, in addition, sharing of spatial datasets and services between public authorities with no restrictions or practical obstacles to its reuse. This data should be published with as few restrictions as possible and clear licences for its use to allow better scrutiny of administrations' decision-making processes and realise transparency in practice. Open data is discussed in more detail in section 4.3.4.

[7] Directive 2003/98/EC and as revised by Directive 2013/37/EU.
[8] Directive 2007/2/EC establishing an Infrastructure for Spatial Information in the European Community (INSPIRE). The recent REFIT evaluation (COM(2016)478 and SWD(2016)273) has shown that there are still serious obstacles to the principle of openness throughout the EU.

Recommendation 2:

Publish the data you own as open data unless certain restrictions apply.

The use of **open source software technologies and products** can help save development cost, avoid a lock-in effect and allow fast adaptation to specific business needs because the developer communities that support them are constantly adapting them. Public administrations should not only use open source software but whenever possible contribute to the pertinent developer communities. Open source is an enabler of the underlying EIF principle on **reusability**.

Recommendation 3:

Ensure a level playing field for open source software and demonstrate active and fair consideration of using open source software, taking into account the total cost of ownership of the solution.

The **level of openness of a specification/standard** is decisive for the reuse of software components implementing that specification. This also applies when such components are used to introduce new European public services. If the **openness** principle applies in full:

- all stakeholders have the opportunity to contribute to the development of the specification and a public review is part of the decision-making process;
- the specification is available for everyone to study;
- intellectual property rights to the specification are licensed on FRAND[9] terms, in a way that allows implementation in both proprietary and open source software, [10] and preferably on a royalty-free basis.

Due to their positive effect on interoperability, the use of open specifications has been promoted in many policy statements and is encouraged for European public service delivery. The positive effect of open specifications is demonstrated by the internet ecosystem. However, public administrations may decide to use less open specifications if open ones do not exist or do not meet functional needs. In all cases, specifications should be mature and sufficiently supported by the market, unless they are being used to create innovative solutions.

[9] FRAND: fair, reasonable and non-discriminatory.
[10] This fosters competition since providers working under various business models may compete to deliver products, technologies and services based on such specifications.

Recommendation 4:

Give preference to open specifications, taking due account of the coverage of functional needs, maturity and market support and innovation.

Lastly, openness also means empowering citizens and businesses to get involved in the design of new services, to contribute to service improvement and to give feedback about the quality of the existing public services.

2.4 Underlying principle 3: transparency

Transparency in the EIF context refers to:

i. Enabling **visibility** inside the administrative environment of a public administration. This is about allowing other public administrations, citizens and businesses to view and understand administrative rules, processes,[11] data, services and decision-making.

ii. Ensuring **availability of interfaces** with internal information systems. Public administrations operate a large number of what are often heterogeneous and disparate information systems in support of their internal processes. Interoperability depends on ensuring the availability of interfaces to these systems and the data they handle. In turn, interoperability facilitates reuse of systems and data, and enables these to be integrated into larger systems.

iii. Securing the right to the **protection of personal data**, by respecting the applicable legal framework for the large volumes of personal data of citizens, held and managed by Public administrations.

Recommendation 5:

Ensure internal visibility and provide external interfaces for European public services.

2.5 Underlying principle 4: reusability

Reuse means that public administrations confronted with a specific problem seek to benefit from the work of others by looking at what is available, assessing its usefulness or relevance to the problem at hand, and where appropriate, adopting solutions that have proven their value elsewhere. This requires the public administration to be open to sharing its interoperability solutions, concepts, frameworks, specifications, tools and components with others.

[11] For example, with the establishment of the Digital Single Gateway, a DSM action.

Reusability of IT solutions (e.g. software components, Application Programming Interfaces, standards), information and data, is an enabler of interoperability and improves quality because it extends operational use, as well as saving money and time. This makes it a major contributor to the development of a digital single market in the EU. Some EU standards and specifications also exist in the DIFs and should be applied more widely. For example, the INSPIRE Directive sets out interoperability standards for addresses, cadastres, roads and many other data topics of relevance to many public administrations. These existing standards and specifications can and should be used more widely beyond the domain for which they were originally developed.

Several public administrations and governments across the EU already promote sharing and reuse of IT solutions by adopting new business models, promoting the use of open source software for key ICT services and when deploying digital service infrastructure.

There are some key challenges that limit the sharing and reuse of IT solutions, at technical, organisational, legal and communication levels. The ISA² sharing and reuse framework for IT solutions[12] provides recommendations for public administrations to help them overcome these challenges and share/reuse common IT solutions. Reuse and sharing can be effectively supported by collaborative platforms.[13]

Recommendation 6:

Reuse and share solutions, and cooperate in the development of joint solutions when implementing European public services.

Recommendation 7:

Reuse and share information and data when implementing European public services, unless certain privacy or confidentiality restrictions apply.

2.6 Underlying principle 5: technological neutrality and data portability

When establishing European public services, public administrations should focus on functional needs and defer decisions on technology as long as possible in order to minimise technological dependencies, to avoid imposing specific technical implementations or products on their constituents and to be able to adapt to the rapidly evolving technological environment.

[12] https://joinup.ec.europa.eu/community/isa/document/sharing-and-reuse-framework-fostering-collaboration-among-public-administrati

[13] At EU level, the Joinup platform (https://joinup.ec.europa.eu/) has been set up to share open source software components, semantic assets, building blocks and best practices. The European Commission has also introduced the EUPL licence to encourage sharing of software components.

Public administrations should provide for access and reuse of their public services and data **irrespective of specific technologies or products**.

Recommendation 8:

Do not impose any technological solutions on citizens, businesses and other administrations that are technology-specific or disproportionate to their real needs.

The functioning of the digital single market requires data to be easily transferable among different systems to avoid lock-in, support the free movement of data. This requirement relates to **data portability** - the ability to move and reuse data easily among different applications and systems**,** which becomes even more challenging in cross-border scenarios.

Recommendation 9:

Ensure data portability, namely that data is easily transferable between systems and applications supporting the implementation and evolution of European public services without unjustified restrictions, if legally possible.

2.7 Underlying principle 6: user-centricity

Users of European public services are meant to be any public administration, citizen or businesses accessing and benefiting from the use of these services. Users' needs should be considered when determining which public services should be provided and how they should be delivered.

Therefore, as far as possible, user needs and requirements should guide the design and development of public services, in accordance with the following expectations:

- A **multi-channel** service delivery approach, meaning the availability of alternative channels, physical and digital, to access a service, is an important part of public service design, as users may prefer different channels depending on the circumstances and their needs;
- A **single point of contact** should be made available to users, to hide internal administrative complexity and facilitate access to public services, e.g. when multiple bodies have to work together to provide a public service;
- **Users' feedback** should be systematically collected, assessed and used to design new public services and to further improve existing ones;

- As far as possible, under the legislation in force, users should be able to provide data **once only,** and administrations should be able to retrieve and share this data to serve the user, in accordance with data protection rules;
- Users should be asked to provide only the **information that is absolutely necessary** to obtain a given public service.

Recommendation 10:

Use multiple channels to provide the European public service, to ensure that users can select the channel that best suits their needs.

Recommendation 11:

Provide a single point of contact in order to hide internal administrative complexity and facilitate users' access to European public services.

Recommendation 12:

Put in place mechanisms to involve users in analysis, design, assessment and further development of European public services.

Recommendation 13:

As far as possible under the legislation in force, ask users of European public services once-only and relevant-only information.

2.8 Underlying principle 7: inclusion and accessibility

Inclusion is about enabling everyone to take full advantage of the opportunities offered by new technologies to access and make use of European public services, overcoming social and economic divides and exclusion.

Accessibility ensures that people with disabilities, the elderly and other disadvantaged groups can use public services at service levels comparable to those provided to other citizens.[14]

Inclusion and accessibility must be part of the whole development lifecycle of a European public service in terms of design, information content and delivery. It should comply with e-accessibility specifications widely recognised at European or international level.[15]

[14] Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of websites and mobile applications of public sector bodies, and work launched by the Commission on a 'European Accessibility Act'.

Inclusion and accessibility usually involve multi-channel delivery. Traditional paper-based or face-to-face service delivery may need to co-exist with electronic delivery.

Inclusion and accessibility can also be improved by an information system's ability to allow third parties to act on behalf of citizens who are unable, either permanently or temporarily, to make direct use of public services.

Recommendation 14:

Ensure that all European public services are accessible to all citizens, including persons with disabilities, the elderly and other disadvantaged groups. For digital public services, public administrations should comply with e-accessibility specifications that are widely recognised at European or international level.

2.9 Underlying principle 8: security and privacy

Citizens and businesses must be confident that when they interact with public authorities they are doing so in a **secure** and trustworthy environment and in full compliance with relevant regulations, e.g. the Regulation and Directive on data protection,[16] and the Regulation on electronic identification and trust services.[17] Public administrations must guarantee the citizens' **privacy**, and the confidentiality, authenticity, integrity and non-repudiation of information provided by citizens and businesses. Security and privacy are discussed in more detail in section 4.3.7.

Recommendation *15:*

Define a common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

2.10 Underlying principle 9: multilingualism

European public services can potentially be used by anyone in any Member State. So multilingualism needs to be carefully considered when designing them. Citizens across

[15] See also EC standardisation mandate No 376 on the development of European standards for public procurement of accessible ICT products and services.
[16] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.
[17] Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market**.**

Europe often have problems in accessing and using digital public services if these are not available in the languages they speak.

A balance needs to be found between the expectations of citizens and businesses to be served in their own language(s) or their preferred language(s) and the ability of Member States' public administrations to offer services in all official EU languages. A suitable balance could be that European public services are available in the languages of the expected end-users, i.e. the number of languages is decided on the basis of users' needs, such as the level to which the service is critical for the implementation of the digital single market or national policies, or the size of the relevant audience.

Multilingualism comes into play not just in the user interface, but at all levels in the design of European public services. For example, the choices made on data representation in an electronic database should not limit its ability to support different languages.

The multilingual aspect of interoperability becomes also relevant when a public service requires exchanges between information systems across language boundaries, as the meaning of the information exchanged must be preserved.

Recommendation 16:

Use information systems and technical architectures that cater for multilingualism when establishing a European public service. Decide on the level of multilingualism support based on the needs of the expected users.

2.11 Underlying principle 10: administrative simplification

Where possible, public administrations should seek to streamline and simplify their administrative processes by improving them or eliminating any that does not provide public value. Administrative simplification can help businesses and citizens to reduce the **administrative burden** of complying with EU legislation or national obligations. Likewise, public administrations should introduce European public services supported by electronic means, including their interactions with other public administrations, citizens and businesses.

Digitisation of public services should take place in accordance with the following concepts:

- **digital-by-default**, whenever appropriate, so that there is at least one digital channel available for accessing and using a given European public service;
- **digital-first** which means that priority is given to using public services via digital channels while applying the multi-channel delivery concept and the no-wrong-door policy, i.e. physical and digital channels co-exist.

Recommendation 17:

Simplify processes and use digital channels whenever appropriate for the delivery of European public services, to respond promptly and with high quality to users' requests and reduce the administrative burden on public administrations, businesses and citizens.

2.12 Underlying principle 11: preservation of information

Legislation requires that decisions and data are stored and can be accessed for a specified time. This means that records [18] and information in electronic form held by public administrations for the purpose of documenting procedures and decisions must be preserved and be converted, where necessary, to new media when old media become obsolete. The goal is to ensure that records and other forms of information keep their legibility, reliability and integrity and can be accessed as long as needed subject to security and privacy provisions.

To guarantee the long-term preservation of electronic records and other kinds of information, formats should be chosen to ensure long-term accessibility, including preservation of associated electronic signatures or seals. In this regard, the use of qualified preservation services, in line with Regulation (EU) 910/2014, can ensure the long-term preservation of information.

For information sources owned and managed by national administrations, preservation is a purely national matter. For information that is not strictly national, preservation becomes a European issue. In that case, an appropriate **'preservation policy'** should be applied by the Member States concerned, to cope with any difficulties arising if the relevant information is used under different jurisdictions.

Recommendation 18:

Formulate a long-term preservation policy for information related to European public services and especially for information that is exchanged across borders.

2.13 Underlying principle 12: assessment of effectiveness and efficiency

There are many ways to take stock of the value of interoperable European public services, including considerations such as return on investment, total cost of ownership, level of

[18] As defined by the second version of the model requirements for the management of electronic records (MoReq2): a record is 'information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of businesses.

flexibility and adaptability, reduced administrative burden, efficiency, reduced risk, transparency, simplification, improved working methods, and level of user satisfaction.

Various technological solutions [19] should be evaluated when striving to ensure the effectiveness and efficiency of a European public service.

Recommendation 19:

Evaluate the effectiveness and efficiency of different interoperability solutions and technological options considering user needs, proportionality and balance between costs and benefits.

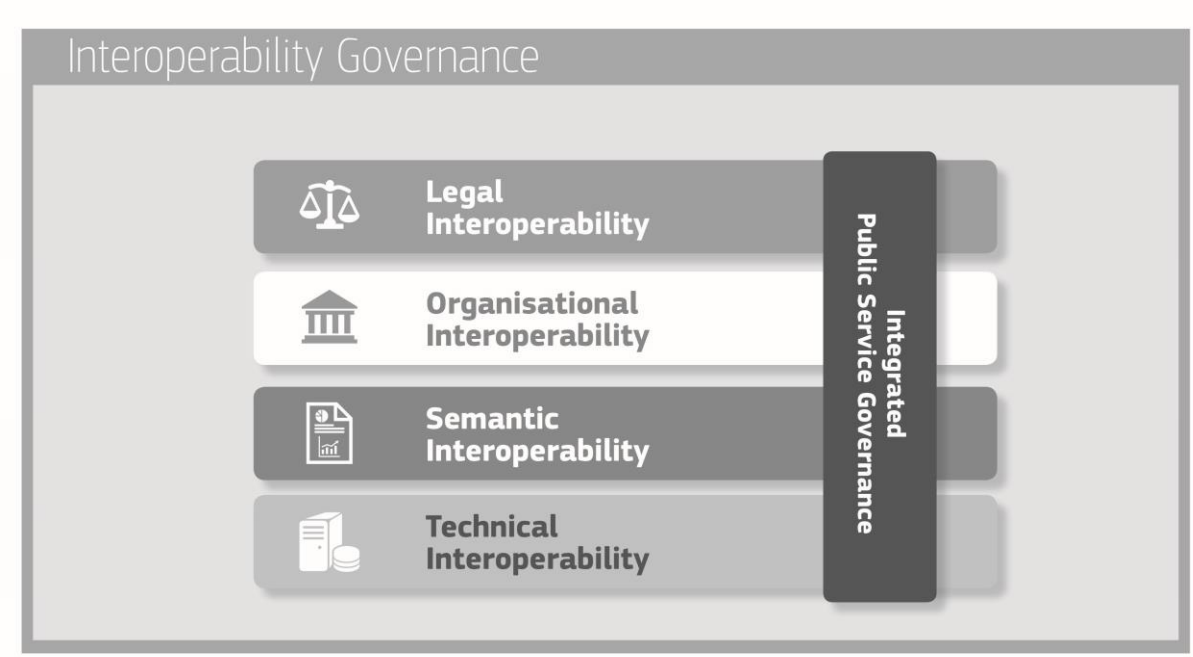
3 INTEROPERABILITY LAYERS

This chapter describes an ***interoperability model*** which is applicable to all digital public services and may also be considered as an integral element of the **interoperability-by-design** paradigm. It includes:

- **four layers** of interoperability: legal, organisational, semantic and technical;
- a cross-cutting component of the four layers, '**integrated public service governance**';
- a background layer, '**interoperability governance**'.

The model is depicted below:

Figure 3: Interoperability model



[19] e.g. cloud computing, Internet of Things, big data, and software-as-a-service.

3.1 Interoperability governance

Interoperability governance refers to decisions on interoperability frameworks, institutional arrangements, organisational structures, roles and responsibilities, policies, agreements and other aspects of ensuring and monitoring interoperability at national and EU levels.

The European interoperability framework, the Interoperability Action Plan (Annex 1 to the Communication) and the European interoperability architecture (EIRA) are important parts of interoperability governance at the EU level.

The INSPIRE Directive is an important domain-specific illustration[20] of an interoperability framework including legal interoperability, coordination structures and technical interoperability arrangements.

European public services operate in a complex and changing environment. Political support is necessary for cross-sectoral and/or cross-border interoperability efforts to facilitate cooperation between public administrations.[21] For effective cooperation, all stakeholders must share a vision, agree on objectives and timeframes and align priorities. Interoperability between public administrations at different administrative levels will only be successful if governments give sufficient priority and assign resources to their respective interoperability efforts.[22]

The lack of the necessary in-house skill sets is another barrier to implementing interoperability policies. Member States should include interoperability skills in their interoperability strategies, acknowledging that interoperability is a multi-dimensional issue that needs awareness and skills in legal, organisational, semantic and technical.

The implementation and delivery of a given European public service often relies on components that are common to many European public services. The sustainability of these components, which are covered by interoperability agreements reached outside the scope of a particular European public service, should be guaranteed over time. This is fundamental, as interoperability should be guaranteed in a sustainable way and not as a one-off target or project. As common components and interoperability agreements are the results of work done by public administrations at different levels (local, regional, national, and EU), coordination and monitoring requires a holistic approach.

[20] Article 1 of the INSPIRE Directive restricts its scope to 'the purposes of Community environmental policies or activities which may have an impact on the environment'.
[21] The ISA² programme is an example of such political support.
[22] See for example the Report from the Commission to the Council and the European Parliament on the implementation of Directive 2007/2/EC of March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE) pursuant to Article 23, 2016.

Interoperability governance is the key to a **holistic approach** on interoperability, as it brings together all the instruments needed to apply it.

Recommendation 20:

Ensure holistic governance of interoperability activities across administrative levels and sectors.

Coordination, communication and monitoring are of the utmost importance for successful governance. The European Commission, through the ISA[2] programme, supports a **National Interoperability Framework Observatory (NIFO).** Its main objective is to provide information about NIFs and related interoperability and digital strategies/policies, to help public administrations share and reuse experiences and to support the **'transposition'** of the EIF nationally. A NIF can be one or more documents that define frameworks, policies, strategies, guidelines and action plans on interoperability in a Member State.

3.1.1 Identifying and selecting standards and specifications

Standards and specifications are fundamental to interoperability. There are six steps to managing them appropriately:

- **identifying** candidate standards and specifications based upon specific needs and requirements;
- **assessing** candidate standards and specifications using standardised, transparent, fair and non-discriminatory methods;[23]
- **implementing** the standards and specifications according to plans and practical guidelines;
- **monitoring** compliance[24] with the standards and specifications;
- **managing change** with appropriate procedures;
- **documenting** standards and specifications, in open catalogues, using a standardised description.[25]

[23] For example the common assessment method for standards and specifications (CAMSS) developed in the context of the ISA programme.
[24] Compliance models could include options like mandatory, comply-or-explain, good-to-have, optional, etc.
[25] For example the asset description metadata schema (ADMS) developed in the context of the ISA programme.

Recommendation 21:

Put in place processes to select relevant standards and specifications, evaluate them, monitor their implementation, check compliance and test their interoperability.

Recommendation 22:

Use a structured, transparent, objective and common approach to assessing and selecting standards and specifications. Take into account relevant EU recommendations and seek to make the approach consistent across borders.

Recommendation 23:

Consult relevant catalogues of standards, specifications and guidelines at national and EU level, in accordance with your NIF and relevant DIFs, when procuring and developing ICT solutions.

Standards and specifications can be mapped to the EIRA and catalogued in the European interoperability cartography (EIC).

In some cases, public administrations may find that no suitable standards/specifications are available for a specific need in a specific domain. Active participation in the standardisation process mitigates concerns about delays, improves the alignment of standards and specifications with public sector needs and can help governments keep pace with technological innovation.

Recommendation 24:

Actively participate in standardisation work relevant to your needs to ensure your requirements are met.

3.2 Integrated public service governance

European public service provision often requires different public administrations to work together to meet end users' needs and provide **public services in an integrated way**. When multiple organisations are involved there is a need for coordination and governance by the authorities with a mandate for planning, implementing and operating European public services. Services should be governed to ensure: integration, seamless execution, reuse of

services and data, and development of new services and '**building blocks'**.[26] More is said about the aspects of **'integrated public service provision'** in section 4.3.1.

Focusing here on the governance part, this should cover all layers: legal, organisational, semantic and technical. Ensuring interoperability when preparing legal instruments, organisation business processes, information exchange, services and components that support European public services is a continuous task, as interoperability is regularly disrupted by changes to the environment, i.e. in legislation, the needs of businesses or citizens, the organisational structure of public administrations, the business processes, and by the emergence of new technologies. It requires, among other things, organisational structures and roles and responsibilities for the delivery and operation of public services, service level agreements, establishment and management of interoperability agreements, change management procedures, and plans for business continuity and data quality.

Integrated public service governance should include as a minimum:

- the definition of **organisational structures**, **roles & responsibilities** and the **decision-making process** for the stakeholders involved;
- the imposition of **requirements** for:
    - aspects of interoperability including quality, scalability and availability of reusable building blocks including information sources (base registries, open data portals, etc.) and other interconnected services;
    - external information/services, translated into clear service level agreements (including on interoperability);
- a **change management** plan, to define the procedures and processes needed to deal with and control changes;
- a **business continuity/disaster recovery plan** to ensure that digital public services and their building blocks continue to work in a range of situations, e.g. cyberattacks or the failure of building blocks.

Recommendation 25:

Ensure interoperability and coordination over time when operating and delivering integrated public services by putting in place the necessary governance structure.

[26] A 'building block' is a self-contained, interoperable and replaceable unit encapsulating an internal structure.

3.2.1 Interoperability agreements

Organisations involved in European public service provision should make **formal arrangements** for cooperation through **interoperability agreements**. Setting up and managing these agreements is part of public service governance.

Agreements should be detailed enough to achieve their aim, i.e. to provide European public services, while leaving each organisation the maximum feasible internal and national autonomy.

At semantic and technical levels, but also in some cases at organisational level, interoperability agreements usually include standards and specifications. At legal level, interoperability agreements are made specific and binding via legislation at EU and/or national level or via bilateral and multilateral agreements.

Other types of agreements can complement interoperability agreements, addressing operational matters. For example, memoranda of understanding (MoUs), service level agreements (SLAs), support/escalation procedures and contact details, referring, if necessary, to underlying agreements at semantic and technical levels.

Since delivering a European public service is the result of collective work with parties that produce or consume parts of the service, it is critical to include appropriate change management processes in the interoperability agreements to ensure the accuracy, reliability, continuity and evolution of the service delivered to other public administrations, businesses and citizens.

Recommendation 26:

Establish interoperability agreements in all layers, complemented by operational agreements and change management procedures.

3.3 Legal interoperability

Each public administration contributing to the provision of a European public service works within its own national legal framework. Legal interoperability is about ensuring that organisations operating under different legal frameworks, policies and strategies are able to work together. This might require that legislation does not block the establishment of European public services within and between Member States and that there are clear agreements about how to deal with differences in legislation across borders, including the option of putting in place new legislation.

The first step towards addressing legal interoperability, is to perform **'interoperability checks'** by screening existing legislation to identify **interoperability barriers**: sectoral or geographical restrictions in the use and storage of data, different and vague data licence models, over-restrictive obligations to use specific digital technologies or delivery modes to provide public services, contradictory requirements for the same or similar business processes, outdated security and data protection needs, etc.

Coherence between legislation, in view of ensuring interoperability, should be assessed before adoption and through evaluating their performance regularly once they are put into application.

Bearing in mind that European public services are clearly meant to be provided - amongst others - from digital channels, ICT must be considered as early as possible in the law-making process. In particular, proposed legislation should undergo a **'digital check'**:

- to ensure that it suits not only the physical but also the digital world (e.g. the internet);
- to identify any barriers to digital exchange; and
- to identify and assess its ICT impact on stakeholders.

This will facilitate interoperability between public services at lower levels (semantic and technical) as well, and increase the potential for reusing existing ICT solutions, so reducing cost and implementation time.

The legal value of any information exchanged between Member States should be maintained across borders, and data protection legislation in both originating and receiving countries complied with. This might require additional agreements to overcome potential differences in the implementation of the applicable legislation.

Recommendation 27:

Ensure that legislation is screened by means of 'interoperability checks', to identify any barriers to interoperability. When drafting legislation to establish a European public service, seek to make it consistent with relevant legislation, perform a 'digital check' and consider data protection requirements.

3.4 Organisational interoperability

This refers to the way in which public administrations align their business processes, responsibilities and expectations to achieve commonly agreed and mutually beneficial goals. In practice, organisational interoperability means documenting and integrating or aligning business processes and relevant information exchanged. Organisational interoperability also

aims to meet the requirements of the user community by making services available, easily identifiable, accessible and user-focused.

3.4.1 Business process alignment

In order for different administrative entities to be able to work together efficiently and effectively to provide European public services, they may need to align their existing business processes or define and establish new ones.

Aligning business processes implies documenting them in an agreed way and with commonly accepted modelling techniques, including the associated information exchanged, so that all public administrations contributing to the delivery of European public services can understand the overall (end-to-end) business process and their role in it.

Recommendation 28:

Document your business processes using commonly accepted modelling techniques and agree on how these processes should be aligned to deliver a European public service.

3.4.2 Organisational relationships

Service orientation, upon which the conceptual model for public services is conceived, means that the relationship between service providers and service consumers must be clearly defined.

This involves finding instruments to formalise mutual assistance, joint action and interconnected business processes as part of service provision e.g. MoUs and SLAs between participating public administrations. For cross-border actions, these should preferably be multilateral or global European agreements.

Recommendation 29:

Clarify and formalise your organisational relationships for establishing and operating European public services.

3.5 Semantic interoperability

Semantic interoperability ensures that the precise format and meaning of exchanged data and information is preserved and understood throughout exchanges between parties, in other words ‘what is sent is what is understood’. In the EIF, semantic interoperability covers both semantic and syntactic aspects:

- **The semantic** aspect refers to the meaning of data elements and the relationship between them. It includes developing vocabularies and schemata to describe data exchanges, and ensures that data elements are understood in the same way by all communicating parties;
- **The syntactic** aspect refers to describing the exact format of the information to be exchanged in terms of grammar and format.

A starting point for improving semantic interoperability is to **perceive data and information as a valuable public asset**.

Recommendation 30:

Perceive data and information as a public asset that should be appropriately generated, collected, managed, shared, protected and preserved.

An information management strategy should be drafted and coordinated at the highest possible level (corporate or enterprise) to avoid fragmentation and set priorities.

For example, agreements on reference data, in the form of taxonomies, controlled vocabularies, thesauri, code lists[27] and reusable data structures/models[28] are key prerequisites for achieving semantic interoperability. Approaches like **data-driven-design**, coupled with **linked data** technologies, are innovative ways of substantially improving semantic interoperability.

Recommendation 31:

Put in place an information management strategy at the highest possible level to avoid fragmentation and duplication. Management of metadata, master data and reference data should be prioritised.

Similarly to the way technical standards have fostered technical interoperability (e.g. network connectivity) for decades now, robust, coherent and universally applicable information standards and specifications are needed to enable meaningful information exchange among European public organisations.[29]

Given the different linguistic, cultural, legal, and administrative environments in the Member States, this interoperability layer poses significant challenges. However, unless

[27] For example the Eurovoc thesaurus and the European skills, competence and occupations (ESCO) taxonomy.
[28] The core person, core business, core location and core public service developed by the ISA Programme are examples of cross-sector, reusable data models.
[29] Peristeras V., 'Semantic Standards: Preventing Waste in the Information Industry', IEEE Intelligent Systems, No 4, July-Aug. 2013, vol. 28, pp: 72-75.

standardisation efforts mature in the semantic interoperability layer, it is difficult to ensure seamless information exchange, free movement of data, and data portability among Member States to support a digital single market in the EU.

Recommendation 32:

Support the establishment of sector-specific and cross-sectoral communities that aim to create open information specifications and encourage relevant communities to share their results on national and European platforms.

3.6 Technical interoperability

This covers the applications and infrastructures linking systems and services. Aspects of technical interoperability include interface specifications, interconnection services, data integration services, data presentation and exchange, and secure communication protocols.

A major obstacle to interoperability arises from legacy systems. Historically, applications and information systems in public administrations were developed in a bottom-up fashion, trying to solve domain-specific and local problems. This resulted in fragmented ICT islands which are difficult to interoperate.

Due to the size of public administration and the fragmentation of ICT solutions, the plethora of legacy systems creates an additional interoperability barrier in the technical layer.

Technical interoperability should be ensured, whenever possible, via the use of formal technical specifications.

Recommendation 33:

Use open specifications, where available, to ensure technical interoperability when establishing European public services.

4 THE CONCEPTUAL MODEL FOR INTEGRATED PUBLIC SERVICES PROVISION

4.1 Introduction

This chapter proposes a ***conceptual model for integrated public services*** to guide their planning, development, operation and maintenance by Member States. It is relevant to all governmental levels, from local to EU. The model is **modular and comprises loosely coupled service components**[30] **interconnected through shared infrastructure.**

[30] Service oriented architecture (SOA) is an implementation of that concept.

Recommendation 34:

Use the conceptual model for European public services to design new services or reengineer existing ones and reuse, whenever possible, existing service and data components.

Public administrations need to identify, negotiate and agree on a common approach to interconnecting service components. This will be done at different national administrative levels according to each country's organisational set-up. Access boundaries for services and information should be defined through interfaces and conditions of access.

There are well-known and widely used technical solutions, e.g. web services, to do this, but implementing them at EU level will require concerted efforts by public administrations, including common or compatible models, standards and agreements on common infrastructure.

Recommendation 35:

Decide on a common scheme for interconnecting loosely coupled service components and put in place and maintain the necessary infrastructure for establishing and maintaining European public services.

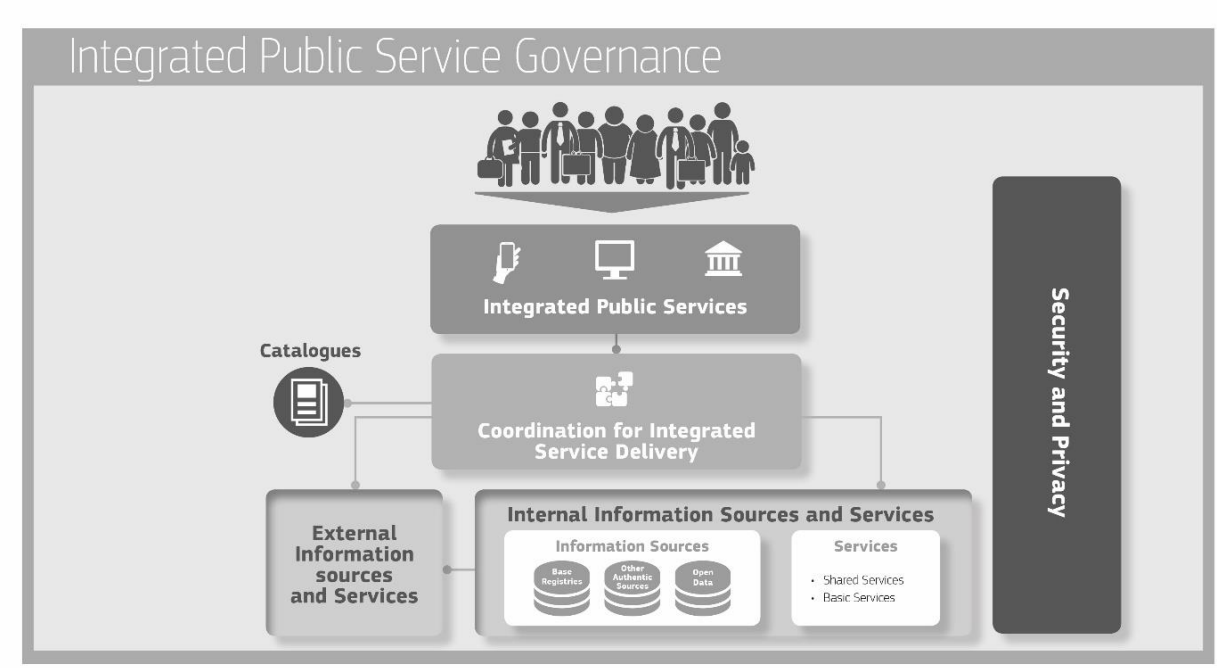
4.2 Model overview

The conceptual model promotes the idea of **interoperability by design**. It means that for European public services to be interoperable, they should be designed in accordance with the proposed model and with certain interoperability and reusability requirements[31] in mind. The model promotes reusability as a driver for interoperability, recognising that the European public services should reuse information and services that already exist and may be available from various sources inside or beyond the organisational boundaries of public administrations. Information and services should be retrievable and be made available in interoperable formats.

The basic components of the conceptual model are presented below.

[31] The interoperability maturity model (IMM) developed in the context of the ISA programme can be used to assess a service's readiness for interoperability.

Figure 4: Conceptual model for integrated public services



The model's structure comprises:

- '**integrated service delivery'** based on a **'coordination function'** to remove complexity for the end-user;
- **a 'no wrong door' service delivery policy,** to provide alternative options and channels for service delivery, while securing the availability of digital channels (digital-by-default);
- **reuse of data and services** to decrease costs and increase service quality and interoperability;
- **catalogues describing reusable services and other assets** to increase their findability and usage;
- **integrated public service governance;**
- **security and privacy**.

4.3 Basic components

4.3.1 Coordination function

The coordination function ensures that needs are identified and appropriate services are invoked and orchestrated to provide a European public service. This function should select the appropriate sources and services and integrate them. Coordination can be automated or

manual. The following process phases are part of **'integrated public service provision'** and executed by the coordination function.

i. **Need identification:** This is prompted by a public service request by a citizen or business.

ii. **Planning:** This entails identifying the services and information sources needed, using the available catalogues, and aggregating them in a single process, considering specific user needs (e.g. personalisation).

iii. **Execution:** This entails collecting and exchanging information, applying business rules (as required by the relevant legislation and policies) to grant or reject access to a service and then providing the requested service to citizens or businesses.

iv. **Evaluation:** After service provision, users' feedback is collected and evaluated.

4.3.2 Internal information sources and services

Public administrations produce and make available a large number of services, while they maintain and manage a huge number and variety of information sources. These information sources are often unknown outside the boundaries of a particular administration (and sometimes even inside those boundaries). The result is duplication of effort and under-exploitation of available resources and solutions.

Information sources (base registries, open data portals, and other authoritative sources of information) and services available not only inside the administrative system but also in the external environment can be used to create integrated public services as building blocks. **Building blocks** (information sources and services) should make their data or functionality accessible using service-oriented approaches.

Recommendation 36:

Develop a shared infrastructure of reusable services and information sources that can be used by all public administrations.

Public administrations should promote policies for sharing services and information sources in three main ways.

i. **Reuse:** When designing new services or revising existing ones, the first step should be to investigate whether existing services and information sources can be reused;

ii. **Publish:** When designing new services and information sources or revising existing ones, reusable services and information sources should be made available to others for reuse;

iii. **Aggregate:** Once appropriate services and information sources are identified, they should be aggregated to form an integrated service provision process. The building blocks should exhibit native capability of being combined ('interoperability by design'), to be ready for mash-up in different environments with minimum customisation. This aggregation is relevant to information, services and other interoperability solutions (e.g. software).

The reusable **building block** approach finds a suitable application by mapping solutions against the conceptual building blocks of a **reference architecture**[32] that allows reusable components to be detected, which also promotes rationalisation. The result of this mapping is a **cartography**[33] of solutions, including their building blocks, that can be reused to serve common business needs and ensure interoperability.

More specifically, to avoid duplication of effort, extra costs and further interoperability problems, while increasing the quality of services offered, the conceptual model features two types of reuse.

- **Reuse of services:** Different types of services can be reused. Examples include basic public services, e.g. issuing a birth certificate, and shared services like electronic identification and electronic signature. Shared services may be provided by the public sector, the private sector or in public-private partnership (PPP) models;
- **Reuse of information:** Public administrations already store large amounts of information with a potential for reuse. Examples include: master data from base registries as authoritative data used by multiple applications and systems; open data under open use licences published by public organisations; other types of authoritative data validated and managed under the aegis of public authorities. Base registries and open data are discussed in more detail in the next section.

4.3.3 Base registries

Base registries are the cornerstone of European public service delivery. A base registry is a trusted and authoritative source of information which can and should be digitally reused by others, where one organisation is responsible and accountable for the collection, use, updating and preservation of information. Base registries are reliable sources of basic information on data items such as people, companies, vehicles, licences, buildings, locations and roads. This type of information constitutes the **'master data'** for public administrations and European public service delivery. 'Authoritative' here means that a base registry is considered to be the

[32] For example the European interoperability reference Architecture (EIRA).
[33] At European level, the European interoperability cartography (EIC), available via the Joinup platform, is a valuable tool for identifying reusable interoperability solutions.

'source' of information, i.e. it shows the correct status, is up-to-date and is of the highest possible quality and integrity.

In case of centralised registries, a single organisational entity is responsible and accountable for ensuring data quality and for having measures in place to ensure the correctness of the data. Such registries are under the legal control of public administrations, whereas operation and maintenance can be outsourced to other organisations if required. There are several types of base registries, e.g. population, businesses, vehicles, cadastres. For the administrations, it is important to obtain a high level overview of the operation of base registries and of the data they store (a registry of registries).

In case of distributed registries there must be a single organisational entity responsible and accountable for every part of the register. Additionally a single entity must be responsible and accountable for the coordination of all parts of the distributed registry.

A **base registry framework**, 'describes the agreements and infrastructure for operating base registries and the relationships with other entities'.

Access to base registries should be regulated to comply with privacy and other regulations; base registries are governed by the principles of information stewardship.

The **information steward** is the body (or possibly individual) responsible and accountable for collecting, using, updating, maintaining and deleting information. This includes defining permissible information use, complying with privacy regulations and security policies, ensuring that information is current and ensuring the accessibility of data by authorised users.

Base registries should draw up and implement a **data quality assurance plan** to ensure the quality of their data. Citizens and businesses should be able to check the accuracy, correctness and completeness of any of their data contained in base registries.

A guide to the terminology used and/or a **glossary** of relevant terms used in each base registry should be made available for both human and machine-readable information purposes.

Recommendation 37:

Make authoritative sources of information available to others while implementing access and control mechanisms to ensure security and privacy in accordance with the relevant legislation.

Recommendation 38:

Develop interfaces with base registries and authoritative sources of information, publish the semantic and technical means and documentation needed for others to connect and reuse available information.

Recommendation 39:

Match each base registry with appropriate metadata including the description of its content, service assurance and responsibilities, the type of master data it keeps, conditions of access and the relevant licences, terminology, a glossary, and information about any master data it uses from other base registries.

Recommendation 40:

Create and follow data quality assurance plans for base registries and related master data.

4.3.4 Open data

The Directive on the reuse of public sector information provides a common legal framework for reuse of public sector data. The focus is on releasing **machine-readable** data for use by others to stimulate transparency, fair competition, innovation and a **data-driven economy**. To ensure a level playing field, the opening and reuse of data must be non-discriminatory, meaning that data must be interoperable so that can be found, discovered and processed.

Recommendation 41:

Establish procedures and processes to integrate the opening of data in your common business processes, working routines, and in the development of new information systems.

There are currently many barriers to the use of open data. It is often published in different formats or formats that hinder easy use, it can lack appropriate metadata, the data itself can be of low quality, etc. Ideally **basic metadata**[34] and the semantics of **open datasets** should be described in a standard format readable by machines.

[34] For example those included in the DCAT-AP specification developed in the context of the ISA programme.

Recommendation 42:

Publish open data in machine-readable, non-proprietary formats. Ensure that open data is accompanied by high quality, machine-readable metadata in non-proprietary formats, including a description of their content, the way data is collected and its level of quality and the licence terms under which it is made available. The use of common vocabularies for expressing metadata is recommended.

Data can be used in different ways and for various purposes and open data publishing should allow this. Nevertheless, users might find problems with datasets or might comment on their quality or might prefer other ways of publishing. Feedback loops can help in learning more about the way datasets are used and how to improve their publication.

For reuse of open data to reach its full potential, legal interoperability and certainty is essential. For this reason, the right for anyone to reuse open data should be communicated clearly throughout the Member States, and legal regimes to facilitate the reuse of data, such as licences, should as far as possible be promoted and standardised.

Recommendation 43:

Communicate clearly the right to access and reuse open data. The legal regimes for facilitating access and reuse, such as licences, should be standardised as much as possible.

4.3.5 Catalogues

Catalogues help others to find reusable resources (e.g. services, data, software, data models). Various types of catalogue exist, e.g. directories of services, libraries of software components, open data portals, registries of base registries, metadata catalogues, catalogues of standards, specifications and guidelines. Commonly agreed descriptions of the services, data, registries and interoperable solutions published in catalogues are needed to enable interoperability between catalogues.[35] A specific kind of catalogue is the **European interoperability cartography (EIC)** of interoperability solutions available for reuse and sharing.

[35] The DCAT-AP, the Core Public Service Vocabulary and the Asset Description Metadata Schema are examples of specifications used to describe open data, public services and interoperability solutions respectively. For example: GeoDCAT-AP is an extension of DCAT-AP for describing geospatial datasets, dataset series, and services. It provides an RDF syntax binding for the union of metadata elements defined in the core profile of ISO 19115:2003 and those defined in the framework of the INSPIRE Directive.

Recommendation 44:

Put in place catalogues of public services, public data, and interoperability solutions and use common models for describing them.

4.3.6 External information sources and services

Public administrations need to exploit services delivered outside their organisational boundaries by third parties, such as payment services provided by financial institutions or connectivity services provided by telecommunications providers. They need also to exploit external information sources such as open data and data from international organisations, chambers of commerce, etc. Moreover, useful data can be collected through the Internet of Things (e.g. sensors) and social web applications.

Recommendation 45:

Where useful and feasible to do so, use external information sources and services while developing European public services.

4.3.7 Security and privacy

Security and privacy are primary concerns in the provision of public services. Public administrations should ensure that:

- they follow the **privacy-by-design** and **security-by-design** approach to secure their complete infrastructure and building blocks;
- services **are not vulnerable to attacks** which might interrupt their operation and cause data theft or data damage; and
- they are compliant with the legal requirements and obligations regarding **data protection and privacy** acknowledging the risks to privacy from advanced data processing and analytics.

They should also ensure that controllers comply with data protection legislation, by covering the following points.

- **'Risk management plans'** to identify risks, assess their potential impact and plan responses with appropriate technical and organisational measures. Based on the latest technological developments, those measures must ensure that the level of security is commensurate with the degree of risk;

- **'Business continuity plans'** and **'Back-up and recovery plans' to** put in place the procedures needed for functions to operate after a disastrous event and bring all functions back to normal the earliest possible;
- A **'data access and authorisation plan'** which determines who has access to what data and under what conditions, to ensure privacy. Unauthorised access and security breaches should be monitored and appropriate actions should be taken to prevent any recurrence of breaches;
- Use of **qualified trust services** in line with the **eIDAS regulation**[36] to ensure the integrity, authenticity, confidentiality and non-repudiation of data.

When public administrations and other entities exchange official information, the information should be transferred, depending on security requirements, via a secure, harmonised, managed and controlled network.[37] Transfer mechanisms should facilitate information exchanges between administrations, businesses and citizens that are:

- **registered and verified**, so that both sender and receiver have been identified and authenticated through agreed procedures and mechanisms;
- **encrypted**, so that the confidentiality of the exchanged data is ensured;
- **time stamped**, to maintain accurate time of electronic records' transfer and access;
- **logged**, for electronic records to be archived, thus ensuring a legal audit trail.

Appropriate mechanisms should allow secure exchange of electronically verified messages, records, forms and other kinds of information between the different systems; should handle specific security requirements and electronic identification and trust services such as electronic signatures/seals creation and verification; and should monitor traffic to detect intrusions, changes of data and other type of attacks.

Information must also be appropriately protected during transmission, processing and storage by different security processes such as:

- defining and applying security policies;
- security training and awareness;
- physical security (including access control);
- security in development;
- security in operations (including security monitoring, incident handling, vulnerability management);

[36] Regulation (EU) No 910/ 2014.
[37] For example the TestaNG secured network.

- security reviews (including audits and technical checks).

As data from different Member States may be subject to different data protection implementation approaches, common requirements for data protection should be agreed before providing aggregated services.

The provision of secure data exchange also requires several management functions, including:

- **service management** to oversee all communications on identification, authentication, authorisation, data transport, etc., including access authorisations, revocation and audit;
- **service registration** to provide, subject to proper authorisation, access to available services through prior localisation and verification that the service is trustworthy;
- **service logging** to ensure that all data exchanges are logged for future reference and archived when necessary.

Recommendation 46:

Consider the specific security and privacy requirements and identify measures for the provision of each public service according to risk management plans.

Recommendation 47:

Use trust services according to the Regulation on eID and Trust Services as mechanisms that ensure secure and protected data exchange in public services.

5 CONCLUSION

In recent decades, European public administrations have invested in ICT to modernise their internal operations, reduce costs and improve the services they offer to citizens and businesses. Despite the significant progress made and benefits obtained already, administrations still face considerable barriers to exchanging information and collaborating electronically. These include legislative barriers, incompatible business processes and information models, and the diversity of technologies used. This is because, historically, information systems were set up in the public sector independently of each other and not in a coordinated way. The diversity of institutional configurations across Europe adds another layer of complexity at EU level.

Interoperability is a prerequisite for enabling electronic communication and exchange of information between public administrations. This makes it also a prerequisite for achieving a digital single market. Interoperability programmes in the EU have evolved over time. At first,

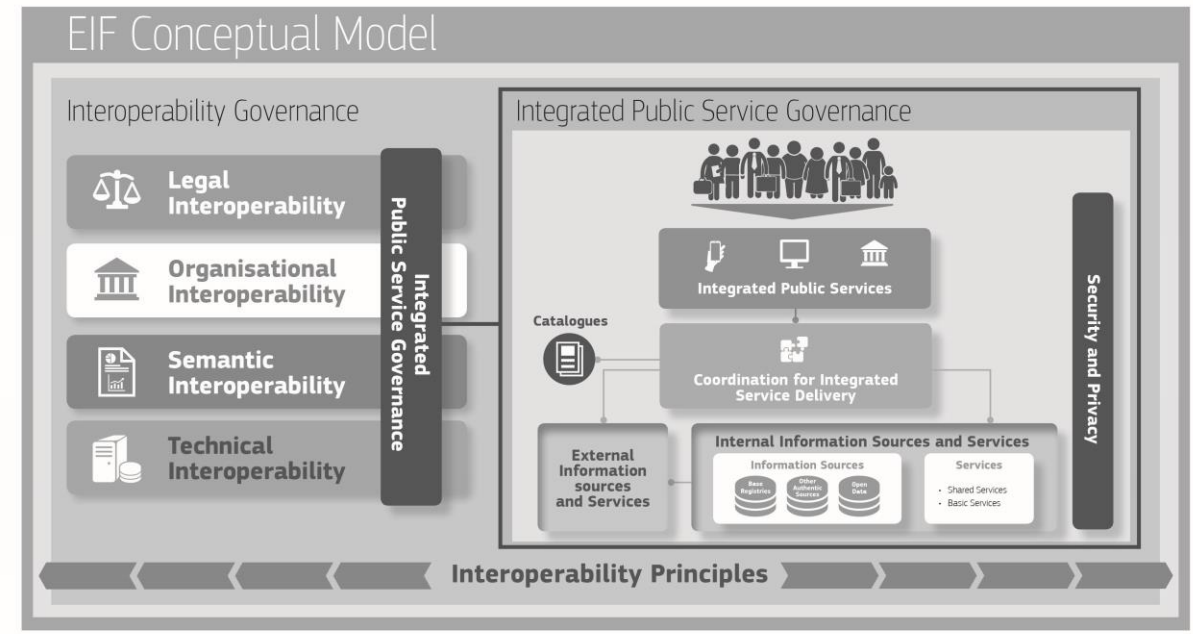
they were concerned with achieving interoperability in particular domains, then with putting in place common infrastructure. More recently, they have started to address interoperability at the semantic level. Governance, compatibility of legal regimes, alignment of business processes and secure access to data sources are some of the issues to be addressed next, to provide fully fledged public services.

The EIF promotes electronic communication among European public administrations by providing a set of common models, principles and recommendations. It acknowledges and stresses the fact that interoperability is not only an ICT matter, as it has layers of implications ranging from the legal to the technical. Addressing issues in a holistic approach in all these layers and at different administrative levels from local to EU remains a challenge. The EIF identifies four layers of interoperability challenges (legal, organisational, semantic and technical) at the same time pointing out the essential role of governance to ensure coordination of relevant activities across all levels and sectors of administration.

The EIF conceptual model for public services covers the design, planning, development, operation and maintenance of integrated public services at all governmental levels from local to EU level. The principles set out here guide decision-making on establishing interoperable European public services. Moreover, the EIF offers practical tools in the form of a set of actionable recommendations.

The components of the EIF are depicted in Figure 5.

Figure 5: EIF conceptual model relations



The revised EIF is a key instrument for establishing interoperable digital public services at regional, national and EU level, thereby contributing to making the digital single market a reality.

6 ANNEX

6.1 Abbreviations

Abbreviation	Meaning
A2A	Administration to administration
A2B	Administration to business
A2C	Administration to citizen
DIF	Domain-specific interoperability framework
DSM	Digital single market
EC	European Commission
EIC	European interoperability cartography
EIF	European interoperability framework
EIRA	European interoperability reference architecture
EU	European Union
EUPL	European Union public licence
ICT	Information and communication technology
INSPIRE	Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE)
ISA	Interoperability solutions for European public administrations
ISA²	Interoperability solutions and common frameworks for European public administrations, business and citizens
MoU	Memorandum of understanding
MS	Member State
NIF	National interoperability framework
NIFO	National Interoperability Framework Observatory
PSI	Public sector information

SLA	Service level agreement
SOA	Service-oriented architecture