D1.8 Updated legal, technical, cultural and managerial risks and barriers

Document Identification			
Status	Final	**Due Date**	30/09/2022
Version	1.0	**Submission Date**	03/10/2022

Related WP	WP1	**Document Reference**	D1.8
Related Deliverable(s)	WP2, WP6, WP7	**Dissemination Level (*)**	PU
Lead Participant	JSI	**Lead Author**	Tanja Pavleska (JSI)
Contributors	Tanja Pavleska (JSI)	**Reviewers**	Arvid Welin (SU)
			Hans Graux (TLX)

Keywords :
Legal, Organizational, Business, Political, Technical, Human factor, Barriers, OOP implementation, Cross-border

Document Information

List of Contributors	
Name	Partner
Tanja Pavleska	JSI

Document History			
Version	Date	Change editors	Changes
0.1	27/8/2022	Tanja Pavleska (JSI)	Set up a first draft of the structured document
0.2	1/9/2022	Tanja Pavleska (JSI)	Added revised literature overview
0.3	10/9/2022	Tanja Pavleska (JSI)	Added methodological approach
0.4	15/9/2022	Tanja Pavleska (JSI)	Added data visualization and analysis
0.5	19/9/2022	Tanja Pavleska (JSI)	First draft for internal review
0.6	22/9/2022	Tanja Pavleska (JSI)	Implemented remarks from first internal review
0.7	24/9/2022	Tanja Pavleska (JSI)	Implemented remarks from second internal review
0.8	24/09/2022	Tanja Pavleska (JSI)	Delivered to coordinator for final submission
0.9	26/09/2022	Julia Wells (ATOS)	Revision for final submission
1.0	30/09/2022	Ana Piñuela (ATOS)	Version for final submission

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Tanja Pavleska (JSI)	24/09/2022
Quality manager	Julia Wells (ATOS)	26/09/2022
Project Coordinator	Ana Piñuela Marcos (ATOS)	30/09/2022

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
CIO	Chief Information Officer
DESI	Digital Economy and Society Index
DIW	Digital Identity Wallet
DSI	Digital Service Infrastructure
Dx.y	Deliverable number y, belonging to WP number x
EC	European Commission
EFTA	European Free Trade Association
eID	Electronic identity
eIDAS	Electronic Identification, Authentication and Trust Services
EIF	European Interoperability Framework
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and Communication Technologies
IMI	Internal Market Information
MS	Member State
OOP	Once Only Principle
OOTS	Once-Only Technical System
ROI	Return of investment
SCOOP4C	Stakeholder Community Once-Only Principle For Citizens
SDG	Single Digital Gateway
SDGR	Single Digital Gateway Regulation
SEMPER	Secure Electronic Marketplace for Europe
TOOP	The Once Only Project
WP	Work Package

Executive Summary

The concept of a truly single market of digital services for cross-border citizens and businesses holds tremendous potentials in terms of ease of life and economic gains. However, as with any significant change, the process of bringing that concept to life may risk running the gauntlet, if not carefully planned against the realities of the Member States it bridges.

D1.7 supports the development of a single market for digital services by identifying the legal, technical, cultural and managerial risks and barriers on the implementation of cross-border digital public services.

In order to ensure that a relevant spectrum of risks and barriers are identified and properly understood, the study draws upon three different kinds of sources: A survey (henceforth denoted as the WP1 Survey) among the Chief Information Officers of the EU and EFTA Member States, a desktop research overviewing the relevant literature and practices of European projects / initiatives, and semi-structured expert interviews with EC experts on the topics addressed by the WP1 Survey.

Following a 6-layer generic taxonomy of barriers and drivers as the conceptual framework for this report, we systematize the detected risks, barriers and enablers by their nature and relevance for DE4A context. This enables us to extract relevant recommendations and practical guidelines for a wide set of eGovernment stakeholders.

Detected and described were 104 risks and barriers across the six conceptual layers: legal, technical, organizations, business, political and human factor. For each risk and barrier, a list of enablers in the form of policy recommendation was compiled, amounting to 44 enablers directed at the various eGovernment stakeholder.

Furthermore, the study found that the most prevalent types of barriers that countries face in the implementation of public services are of Legal and Organizational nature, whereas the most critical to address is the Human factor. Lack of resources and lack of expertise are the most painful points from an organizational point of view, and non-harmonized law from a legal point of view. Lack of awareness on availability of services and reluctance to change and adoption are the most critical problems that require immediate action.

Although each risk or barrier may be categorised in some of the six conceptual layers, all factors are intertwined and have implications on the others. This adds further complexity to the effort to output a meaningful recommendation targeted at addressing a particular risks or barriers. At the same time, what is risk in one context, may appear as an enabler in another context.

1 Introduction

1.1 Purpose of the document

In a union of 27 different entities, each with its own historic, administrative, political and financial characteristics and circumstances, initiatives that serve to increase cooperation between the entities and improve mobility for their citizens and businesses must take into account the specificities of each entity in order for it to provide a meaningful and valuable proposition. Especially in a context of political prioritization caused by budgetary restrictions, an initiative must return measurable positive gains commensurate with the cost and complexity of implementation.

The purpose of this report is to support the fulfilment of the ambition of cross-border integrated Digital European Public Services by identifying existing legal, technical, cultural and managerial interoperability barriers on the implementation hereof and by extension the obstacles facing any initiative aiming at digital integration of Member States' services. By identifying these obstacles and the possible drivers and enablers to overcome them, the report provides a knowledge base on which to develop eGovernment initiatives at both national and European level.

The study is one of four designed to chart the current landscape of digitalization in Europe. Hence, this study is a complementary extension of the previous deliverables within the same work package consisting of:

- D1.2 Member State eGovernment Baseline, which elaborates on the current advancement of the existing eGovernment landscape
- D1.4 Member State Once Only and data strategy baseline, which elaborates on the current advancement of data strategy and Once Only implementation
- D1.6 EU Baseline Building Block Catalogue, which identifies the main existing building blocks from EU programmes and projects that can enable Once Only implementation and relevant standard data sharing

In all, the four reports of the work package deliver a comprehensive, multifaceted view on the existing infrastructures, practices, expected benefits and barriers to cross-border digitalization efforts. By doing so, they simultaneously serve as input for the development of the DE4A architecture, pilots and long term business model, and serve the greater purpose of qualifying digitization efforts on national and European scales.

Each of the studies is an update of the previous set of deliverables reporting on the results from the first phase of data gathering.

1.2 Structure of the document

This document is divided into 7 main sections:

- Section 1 (Introduction) gives introductory context and theoretical background to the matter of the deliverable;
- Section 2 (Conceptual framework) elaborates on the theoretical basis of the methodology;
- Section 3 (Empirical framework) introduces the methodology behind the data gathering and its relation to the conceptual framework;
- Section 4 (Survey) presents the results and the analysis of the data gathered through the DE4A survey;
- Section 5 (Inventory of risks and barriers) lists and describes the identified risks and barriers;
- Section 6 (Discussion) discusses the found results in an aggregated format;
- Section 7 (Recommendations) catalogues relevant enablers for each type of barrier, in view of the data analysis and the discussed results;

- Section 8 (Conclusions) provides concluding remarks on the research.

The document additionally includes the following annex:

- Annex: Digital Europe for All (DE4A) survey

1.3 Background

The general overview of eGovernment baseline and the relevant literature and initiatives was elaborated broadly in D1.2. The importance of monitoring and evaluation of the progress of Europe's digital transformation was also stressed and explained. This report is a contribution in that direction, as it aims to bridge the gap between objectives and implementation from the point of view of both the European countries and the Europe's digital agenda.

Risks and barriers often influence several aspects at the same time, appearing in one context as a hurdle, and in another even as an enabler. Regulatory and technological changes are very often such example, causing reluctance for adoption at first, but facilitating all procedures and interactions later. However, such chicken-and-egg intertwining makes it difficult to clearly differentiate between cause and effect.

In order to be able to apply conceptual stringency to the understanding and consequent identification and description of the risks and barriers on the deployment of integrated services, a generic taxonomy of barriers and drivers is followed as the conceptual model for this report. This allows us to systematize the detected risks, barriers and enables us to extract policy recommendations and practical guidelines for a rich set of relevant stakeholders.

Though the concepts of risks, barriers, drivers and enablers may be intuitively understood, for the sake of clarity, especially concerning the differences between the four, the following definitions hold:

- A *risk* is understood as something that may happen and which has a negative effect on the desired outcome if it were to happen.
- A *barrier*, on the other hand, is something which by its current presence or lack thereof has a negative effect on the desired outcome.
- A *driver* is considered as an incentive to make something happen. A driver may have a positive effect on the desired outcome, or counter a negative effect, but it may also have a negative effect on the desired outcome. Examples of this could be generic political or societal changes, or specifically increased costs of supporting manual processes for cross-border services.
- An *enabler* is the opposite of a barrier, i.e. something tangible that may be used or that makes it possible to achieve the desired outcome or parts thereof. Examples of this could be a tool, a building block or the implementation of an initiative or legislation.

As different studies on eGovernment suggest, there is an uneven level of eGovernment advancement across the EU MSs [1]–[4]. Despite the availability of a common regulatory framework and the launch of large-scale cross-border projects, reports on the eGovernment Benchmark demonstrate some countries having a higher rate of eID adoption and availability of public services in a cross-border perspective [1]. The Digital Economy and Society Index similarly depicts unequal coverage of internet connectivity and availability of public digital services across Europe [2]. These differences are essential for comprehension of the current European eGovernment landscape.

In the implementation practice, there are several typologies used to classify and group together different factors affecting digital provision of public services. One early attempt to categorize these factors was made in [5]. According to the authors, factors affecting ICT projects in the public sector can be grouped into five categories: 1) information and data; 2) information technology; 3) organizational and managerial; 4) legal; and 5) institutional and environmental. While the first two concern the availability and quality of data and technology, the remaining three extend beyond the technological domain, relating to the existence of an organizational, legal and institutional environment that

stimulates, or hinders, the provision of digital services. Some examples of these factors are: the size of a project or organizations´ staff, the project alignment with existing goals, the presence of a regulatory framework or incentives; and, finally, pressures from political actors, businesses, or civil society.

Regarding the development of eGovernment in the European Union (EU), in [6] the authors also identified factors from several categories such as technical, legal, social and institutional. In addition to technological/operational aspects, [7] points out the significance of managerial-organizational and political-institutional factors for the adoption of eGovernment services. By observing influential strides of e-procurement in two European regions, the sources of the barriers have also been taken into account, distinguishing between "outer context" and "inner" factors [8]. While the former refers to wider environmental factors, such as economic, social and political factors, as well as the inter-institutional environment and dynamics, inner factors are the ones intrinsically related to the organizations (i.e., organizational, human and technical). The authors also find that political aspects are significant for both contexts. However, they discuss the greater importance of internal over external factors.

Overall, whether examining the provision of e-services, the adoption of ICTs, or eGovernment maturity, the frameworks developed to identify the factors for these outcomes have remained relatively constant and include: legal, political, organizational, business, technical and human determinants. As it will be discussed in the Methodology, these are precisely the dimensions along which we discuss the risks, barriers and enablers for the eGovernment landscape.

Two recurring points can be emphasized from the exhaustive examination focusing on the OOP. The first is that perspectives of individuals, businesses and public officials differ and are often even divergent in terms of perceived barriers to the OOP. The second refers to the importance of the semantic aspects, notably the deviations in data and documents' content and the need for certified translations [9]. The current report pays special attention on the technical factors as barriers and enablers, including the semantics dimension as part of these determinants.

Finally, an important note should be made on the stakeholders as influencing factors. In this, as well as in all other WP1 reports, they are grouped in a high-level taxonomy as "public entities", "private entities" and "citizens". This classification results from the acknowledgment that technology, organizations and institutions cannot account alone for eGovernment and public sector modernization [10]. Being accountable to a number of stakeholders, public sector organizations are highly dependent on political goals and tensions. However, the modernization of services may be highly dependent not only on political will, but also on public and business demands [11]. Hence, citizens and businesses, and their will for adoption of the eGovernment services are a pivotal element of the overall eGovernment landscape. In the case of OOP, the support of political actors and public institutions, the businesses and private companies, as well the civil society, i.e. the citizens, both at national and supranational level, are perceived as a crucial aspect. They are also placed at the core of the analysis in the current report.

Both scholars and experts agree that sharing data across organizations, as well as across national boundaries, reduces administrative burdens and simplifies administrative processes which, in turn, leads to a reduction in time and financial resources required to support those administrative processes. In the same way, the implementation of the OOP, both in terms of principles and as a technical backbone, is seen as a contributor and enabler in and of itself for increased user-friendliness and efficiency of digital service provisions. Moreover, it is also expected to leverage service quality across organizations or countries involved in providing these services [12]. As the results in this report show, the trend of advancement in the eGovernment sector moves precisely in this direction.

One difficulty related to the present report comes from the nature of the survey. In order to capture a holistic picture of the state of eGovernance in a European country, the survey cannot be scattered across contexts and limited only to DE4A-relevant information, risking redundancy of analyzed topics

and questions directed to the CIOs. Being holistic, on the other hand, entails voluminous questionnaires and complex coordination. In addition, it lowers the probability of dataset completeness and, with that, statistical significance of the results. However, we try to strike a balance that alleviates these hurdles and present meaningful analysis by drawing from more data sources and taking an interdisciplinary approach to data analysis.

2 Conceptual framework

2.1 Approach

The purpose of this report is to identify risks and barriers, but also enablers for the implementation of national and cross-border digital European Services. As one of the major objectives of the eGovernance developments in the EU is to be user-centric in their effort to facilitate cross-border access to public services, the development of integrated public services should cater to the needs of all stakeholders from multiple aspects: legal, technological, political, business, political, organizational, and human-oriented. The conceptual derivation of those precise aspects was discussed in the previous section. Here, we investigate on how these aspects were affected in the context of OOP implementation, both at a national and at cross-border levels, and which factors work in inter-dependence to produce the results we uncover through the WP1 survey.

In addition to the WP1 survey as the main data source, the study brings in both internal and external know-how to analyze the results and to investigate related issues and topics. This is done through semi-structured expert interviews, and through a thorough desktop research. The internal factor implies connecting with project-relevant sources (architecture, pilots, legal and governance experts), whereas the external factors means relating to complementary initiatives (EBSI/ESSIF, mGov4EU and TOOP) and relevant EC-experts (DG DIGIT, DG GROW, DG CONNECT). Although the initial plan was to use the results of the study for comparative analysis, together with the results from the first phase, this analysis can be limited to a narrow scope due to several reasons: first, the methodology that was followed in the first phase had to be revised and updated to remove subjectivity and bias, but also to cover the latest development in eGovernment. This led to differences in both the survey and the calculation methodology. Second, the feedback obtained from the Member States does not provide consistent datasets that can be compared even along the same indicators. Not all MSs that contributed to the first phase also provided feedback in the second phase, and those that did have not provided consistent answers. Finally, drawing any conclusion on the progress of DE4A based on this data will make no sense, as the state of eGovernment across Europe depends on many ongoing initiatives with simultaneous, yet separate impact. However, such analysis, in a complete and consistent manner is available from other sources [1] [2].

It is also important to note that this report is not a study that can be used for deriving compliance levels of the EU Member States with the European regulatory and policy frameworks. Neither the nature of the methodological framework nor the quality of the obtained feedback allows for such rigorous statements. At best, the results from this study can be seen as pointers to existing good practices, risks and challenges, drivers and enablers for the European digital transformation goals. The strength of the study in its methodological framework that can be reused and adopted by other future initiatives aiming to contribute to the continuity of digitalization efforts in EU.

The results are mainly represented in an aggregated format, but they also offer a view into some Member States' peculiarities. Making an inventory of the existing eGovernment practices, the report portrays the overall European advancement of the EU Member States, revealing the most crucial developments and pitfalls of the existing European digital space. Based on the obtained results, the study explores the perception of the participating countries of their digital advancement and suggests a ground for further actions.

As a result of the desktop research, the benefits associated with the various eGovernment solutions, but also with the separate drivers and barriers, were identified and used as an input for developing the part of the survey that addresses risks, drivers and barriers. Based on the results of the first phase of data gathering, as well as based on internal consultation with WP1 partners, pilot and task leaders, the inventory of perceived factors was updated and served as an input for refining the conceptual

framework. Hence, the final framework analyses the results along 6 dimensions: Legal, Organizational, Technical, Business, Political, and Human dimension, leaving the possibility to add "Other" factors that influence the national eGovernment landscape, as well as the OOP implementation at a national and cross-border level.

Where the SDGR employs a user-centric focus to ease cross-border users' access to public services, integrated public services may also cater to the needs of the public institutions themselves, e.g. for auditing purposes. As other mechanisms may govern or influence the development of services designed to cater to the needs of the public sector itself, especially legal and organizational mechanisms, risks and barriers may in some respect differ slightly from those on the user-centric services. Different architectural designs may also entail different subsets of risks and barriers, or lead to variations of the identified risks and barriers.

Despite the abovementioned limitations on the direct applicability of all the risks and barriers to every scenario, the services included in the current regulatory framework are treated as representative of the generic concept of cross-border integrated digital public services. By extension, the identification of risks and barriers on the development of those services is then based on the national and European efforts of implementing the SDGR, as they provide unique insight into the actual challenges of developing integrated public services.

Following is a succinct overview of each of the dimensions used as a conception backbone for classifying the risks and barriers, with a view on their relevance for the context of eGovernment.

2.2 Technological Factors

Technological factors bear exclusive relevance in the case of eGovernment due to its reliance on heterogeneous information (types and sources) and organizational models. Technical issues, especially those related to interoperability, are perceived as the most challenging aspects of modern multi-organizational and cross-border information systems [13]. Interoperability, a key element of the OOP technical system, can be defined as the exchange of data between different organizations and their ICT systems. This imposes a requirement for the organizations to have the capacity to interact with each other in order to achieve mutually beneficial and common goals. This becomes especially important on a semantic level, in the case of cooperation between different countries. In addition to the interoperability aspect, in the case of the cross-border context of the OOP, other relevant factors concern data quality, the particularities of various databases or information systems and, finally, countries' overall e-government architecture/infrastructures [9].

Ensuring technical interoperability requires adopting common technical specifications and building infrastructures that enable interconnecting different systems, as well as providing secure data exchange between information systems. Ensuring semantic interoperability requires agreement to common data formats and developing vocabularies to allow communicating systems to understand the meaning of the data in the same way. The EC's concept of interoperability extends beyond technical factors, also covering organizational and legal factors for interoperability. The model on which the EC approach builds is the European Interoperability Framework [14]. The respective factors are put into DE4A context and explained further in the following sections.

2.3 Organizational Factors

The organizational dimension accounts for the significant changes imposed by the OOP implementation in organizational structures and workflows. The required level of collaboration and coordination between different organizations, one of the core aspect of the OOP, is bound to face a number of organizational and administrative barriers affecting organizations' will and capacity to implement OOP [15]. Some of the most common barriers reported so far on the implementation of

OOP at a national level have been: governmental silos and lack of communication between government departments, the complexity of changes in organizational structures, working practices and cultures, and high implementation costs [16]. Another set of barriers that are also very frequently present at a cross-border level are: the importance of organizations' capacity to adapt, transform and innovate, which in turn depends on aspects such as organizational structure and culture, that can also be deemed as human-oriented factors [11]. Finally, the organizations' financial and human resources are one of the most commonly referenced factors for the adoption and successful implementation of electronic services or use of ICTs [17]. The lack of financial, technical and human capacities in an organization are major obstacles to the development of eGovernment.

2.4 Legal Factors

The third dimension of factors affecting the OOP deals with the legislative and institutional aspects. It refers to the sets of rules, laws and principles that may influence the development of the eGovernment landscape [18]. It is common knowledge that public sector organizations are also heavily affected by variables beyond the power of individual organizations, such as the legal culture and administrative traditions of a state. Even though these factors are external to the organizations, and usually more stable, or slower to change, regulations can be determinants for change, and promote innovation by imposing, for example, legal obligations on administrations to implement innovative [11]. Finally, although some directives and regulations have been adopted to support interoperability at the EU level (e.g., Single Digital Gateway Regulation, the Regulation on electronic identification and trust services for electronic transactions – eIDAS, the Services Directive and the General Data Protection Regulation – GDPR), there is still a need to establish a common legal basis at both national and EU level to fully support an EU-wide OOP [9].

2.5 Business factors

The business dimension, although closely related to the organizational in terms of conceptual backbone, brings its own specificities in the set of factors. It represents the private companies and their operational models, mainly joining technology and people in the efforts to maintain those models. As part of the OOP system, it can provide innovative push and faster technological changes, as well as incentives for eGovernment service adoption. However, it can also introduce risks and inhibit the OOP implementation, especially in the case of business model interruption.

2.6 Political factors

The political environment is another critical aspect, with factors such as political stability having a positive effect on the development of eGovernment [19]. Particularly in the case of the OOP, institutional and legal rules are critical for setting limits on data sharing and personal data protection systems. According to [16], resolving any legal obstacles and establishing a sound legal basis is one of the most important strategic issues for implementation of OOP. The role of intergovernmental and supranational institutions is fundamental for the case of the OOP. Either in the role of facilitators in the national context, or as promotors of the national practices at an international level, governments can act as both drivers and inhibitors for the desired changes.

2.7 Human factors

Humans are at the core of all systems, and part of all other dimension as well. All regulatory developments that support the realization of the Europe's digital agenda are user-centric and depend highly on the inclusion of citizens, and on their willingness to adopt new eGovernment services. In addition to the apparent factors of user awareness and digital readiness for e-service adoption, the

human factor is the decisive force behind organizational changes, political will and choice of regulatory models that support the implementation of the OOP. As this report will show, citizens perceptions and actions often go opposite from institutional interests.

3 Empirical framework

In the context of the identified objectives in the previous section, the present study attempts to provide a generalized view on the European eGovernment landscape. To achieve this goal, the conducted research approaches the overall topic from several major points relevant for the European digital space:

- *Electronic Identification and Trust Services (eIDAS)*. The research is composed of three major constituents, namely: electronic identification scheme (eID-schemes), eIDAS-Node and trust services. The findings, on one hand, comprise the general information on the deployed national eID schemes – including their characteristics, participation in the EU cooperation on the eID notification and their actual use indices – and on the other hand, the current status of the eIDAS-Node cross-border interoperability. The findings are complemented by the review of the implementation level of trust services, elaborated in the eIDAS regulation.
- *European Digital Identity Wallets (EU IDW)*. In view of the latest development on eID and the revision of the eIDAS regulation, this part stand at the intersection between eIDAS and the OOP, providing information on the potential transition models present across European countries in the form of (mobile) digital identity wallets.
- *Digital Service Infrastructures (DSI)*. The report reflects the major achievements on implementation of Building Block and sector-specific DSIs, elaborated under the Connecting Europe Facility (CEF) and other EU programs.
- *Single Digital Gateway (SDG).* The research aims to take stock of the existing level of implementation of the essential 21 SGD life events (procedures) for citizens and businesses (as listed in the Annex 2 of the SDG Regulation). The analysis of the implementation level of the SDG life events / procedures is performed from the perspectives of the available authentication method, accessibility for mobile devices (in view of a likely requirement to interact with the EU IDW in the future), compliance with the OOP and availability for cross-border use.

Building on the conceptual framework elaborated in the previous section, we here outline an empirical framework to guide the design of the survey, while addressing the topics relevant for the European digital space.

3.1 Scope

- The geographical scope of the research was covering the 27 Member States of the European Union and was additionally complemented by the 4 EFTA states (Iceland, Liechtenstein, Norway, and Switzerland). The survey questionnaire (see Annex) was sent out to 31 state representatives, covering the aforementioned eGovernment initiatives. Responses were received from 18 countries (17 Member States and 1 EFTA country) - Austria, Belgium, Bulgaria, Croatia, Ireland, Italy, Latvia, Liechtenstein, Luxembourg, Malta, Netherlands, Portugal, Romania, Slovenia, Spain, Sweden, Hungary, and the Czech Republic – amounting to a representativeness of 58% of all (EU+EFTA) countries, and 63% of the Member States.
- Measuring the performance of the EU Member States in the context of the cross-border European initiatives, the research likewise attempts to evaluate the advancement of national eGovernment agenda. Conducting an inventory of the availability of certain eGovernment aspects for national usage, the research investigates the availability of local and regional solutions and approaches toward implementation of the Digital Agenda for Europe [20].

For the second phase of data gathering, several changes were made prior to survey submission:

- First, the survey was revised to lower the amount of subjectivity inserted by the answers in the first phase;
- Second, the topics of interest were revised to match the current EU trends on eGovernance. Thus, the existing survey chapters were revised in terms of redundancy, and an entirely new chapter on Digital Identify Wallets was added.
- Third, the methodology was revised to allow for simpler, yet less subjective data analysis;
- Finally, the overall approach was revised based on the reviewers' comments, the experiences from the first phase of data gathering, and the remarks obtained from internal and external project partners.

It is important to note that the present report should not be seen as an isolated WP1 deliverable, but as piece of a deliverable set whose parts complement each other. Thus, all four deliverables: D1.2, D1.4, D1.6, and D1.8 should be read as a single document.

3.2 Data collection and analysis

Combining both qualitative and quantitative research methods, the study used the following data sources for the assessment of the eGovernment baseline:

- *Data collection survey*. The survey was targeted at the current eGovernment advancement of European states and consisted of 5 major subjects: Electronic Identification and Trust Services, European Digital Identity Wallets, Single Digital Gateway, Digital Service Infrastructures and Once-Only Principle and Data Strategy. The online survey was distributed to the Member States' CIOs of and EFTA countries and the data was collected between March 31st and August 22nd, 2022. The respondents were suggested to also evaluate the performance of their countries with respect to the indicated topics. The questionnaire offered the respondents a possibility to supplement the submitted data with additional comments illustrating country-specific context relevant for understanding the particular eGovernment initiative.
- *Desk research*. The insights derived from the survey are supplemented by the analysis of the existing policies and reports relevant for comprehension of the general eGovernment domain, as well as its advancements along the five topics of interest. The EU policies stipulating development of the shared European digital space have been used as a guideline for survey design and analysis. At the stage of the response analysis, the data obtained via the survey was supported by contextualization of the EU MS' eGovernment development through research of relevant national strategies and legislative frameworks. The results from the survey provide the basis for rich context analysis of the respected country, but more important – for drafting policy recommendations supporting each stakeholder in the process of digital transformation through policy compliance.
- *Semistructured expert interviews*. One of the distinguishing traits of this study compared to the more general overview reports (such as the eGovernment Benchmark reports, the Digital Economy and Society Index (DESI) and NIFO (National Interoperability Framework Observatory), is the ability to obtain information at a more granular level. This information comes from several sources: the DE4A pilots, the architecture iterations in relation to the implementation practices within DE4A, the contextual know-how obtained from the shared experiences with related initiatives (TOOP, SEMPER, BRIS, mGov4EU, etc.), and the dedicated experts interviews on the topics of interests. The results from the latter are integrated into each of the major themes of the survey, enriching the contextual analysis of the survey results. More importantly, the insights from these interviews allow us to view the results from several different perspectives and address the whole spectrum of eGovernance stakeholders.

During pre-processing, survey data was cleansed and checked for consistency. Moreover, contextual information was extracted from the respondents' comments to add relevance to the analysis and to allow for a more granular view of the discussed issues. If needed, direct communication with the respondents was established to clarify the point of either the question or the position response of interest.

One major point that distinguishes this report from the previous (the one delivered from the first phase of data gathering) is the removal of the calculation methodology. The employment of this methodology was deemed as an inappropriate effort for several reasons: first, the methodology was applied to a data containing too subjective answers, making it both inaccurate and inadequate. Second, it was applied to an incomplete dataset and for the purpose of scoring and ranking, which leads to incorrect results.

- *Meaningfulness of the responses*. For the survey targeted at the member states' CIOs, it suggested the respondents to complete the questionnaire at best of their knowledge, leaving out the possibility for abstaining from the answer if the information was not available. Unlike in the first phase, when the answers or choices of "Do not know" and "Not applicable" were not included in the quantitative analysis, these answers are included and considered as relevant to be shown in this phase. The reason for this is that such information also allows to have a closer look into the respondents' engagement with the respective questions as a form of feedback that can trigger additional methodological revisions for any prospective use of this approach.

The results of the study reflect the current advancement of eGovernment of Europe, but the analysis relies to a great extent on the information provided by the CIOs of the European countries. Acknowledging the challenge of gathering multifaceted information on eGovernment performance aggregated at the national level, such approach influences the impartiality of the study. Furthermore, the fact that the survey achieved a response rate of 58% (63% among the Member States), requires to complement the analysis with information from additional sources. Moreover, this data should be consistent methodologically in order to provide the relevant information back up. For similar reasons, the study cannot be assumed to be representative for the complete geographical scope. These drawbacks have been partially overcome by the exhaustive desk research, the context analysis based on the free-text comments in the survey, as well as the semi-structured experts' interviews. The latter is also an argument towards mitigating the risk of biased representation of survey information.

This report has a few limitations. The main one relates to comparability of the country analysis that results both from the second phase and between the two phases. The reason is mainly the incompleteness of data obtained through the surveys and the occasionally low quality of the obtained feedback. In addition, not all countries that provided responses are the same in both phases. However, even if such feedback was perfect in both of the phases, it is not reasonable to draw conclusion about the contributions of DE4A for such outcome, as DE4A is not the only initiative that has been supporting the realization of Europe's eGovernment agenda. Therefore, where available, we support out results with data from other reports as well, but we are cautious when making any comparative analysis, as data comes from different sources and is based on different methodologies.

4 Survey

This chapter addresses different insights into the legal, technical, organizational, business, political and human risks and barriers derived from the DE4A Survey (See Annex). As explained earlier, the analysis is based on data from the survey distributed to the chief information officers of the EU and EFTA countries, which then coordinated the collective feedback for the particular country at a national level. The response rate was 63%, granting the study a sufficiently solid basis for reporting on the actual status of the domains in focus, but implying a cautionary approach in interpreting the results. The first two subsections of this section sublime the findings from the project deliverables D1.2 *Updated Member State eGovernment baseline* and D1.4 *Updated Member State and Once Only and data strategy baseline*. The latter subsections are based on data from the same survey from questions that were posed to specifically inform the current report.

4.1 eGovernment baseline (D1.2)

The eID schemes – the cornerstones for both successful nation-wide digitalization and cross-border functioning of eGovernment systems – have advanced greatly in the last couple of years, especially in terms of their notification status and level of assurance. However, with these advancements came new challenges of a diverse nature. The national eIDAS nodes demonstrate asymmetric, but relatively high readiness for cross-border use, being more advanced in terms of accepting foreign eID-schemes for national use rather than supporting national eIDs abroad. In addition, the implementation of trust services has demonstrated a rather homogenous spread across the participating countries.

The DSIs offered by the Connecting Europe Facility, have likewise showed a different scale of implementation of both domain-specific and domain-independent building blocks. While some DSIs have widely re-used the EU level reference materials, others were not referenced by the majority of the respondent countries. Notably, most of the respondents denoted their on-going Blockchain projects, aiming to increase connectivity and transparency of the built solutions.

The 21 life events announced under the SDG regulation have demonstrated significant progress in terms of the possibility for eID-authentication, mobile accessibility, applicability of the OOP and availability for cross-border use, and less differences in the state of implementation among countries compared to the first phase of the WP1 Survey. In addition to showing generally high availability of the services for use with mobile devices, most of the services were accessible with the eID and enabled for cross-border use. Moreover, the level of digitalization in some or all steps is above 75% for most of the SDG procedures.

From the context-relevant remarks the respondents left on the survey, self-reported dependencies were found of eGovernment initiatives on the administrative system of the country. The peculiarities of the national eGovernment functioning were also complemented by the heterogeneity of the legal environment, revealing a rather incomplete (although more advanced than in the first phase) state of regulatory developments across states. The study also sheds light on the different levels of involvement with the OOP system by the private sector and the citizens, revealing interdependencies with the state of the eGovernment landscape.

4.2 Once Only and data strategy baseline (D1.4)

In regards to data strategy and generic access to base registries, the analysis shows that 81% percent of the responding countries report have in place a strategy for reusing public sector data. Furthermore, most of the base registries are generally accessible by private entities, across most of the respondent countries.

The study also showed that transaction fees are implemented in as much as 62% of the countries for private entities for national use and 42% for cross-border use, as opposed to the 21% and 15% for public entities. In addition to showing uneven legal treatment of public and private entities (including citizens), such a setting could have an adverse effect on the data flows in the OOP technical system, and on achieving the user benefits envisaged by the SDG.

While the study reports a positive picture on citizens' access to data on themselves, the ability for citizens to gain insight into civil servants' access to data appears to be rare. Although current levels of the OOTS implementation appear to be rather low in view of the time horizon for implementing the SDG, noticeable progress has been made in important aspects (legal, technological, and organizational). As differences in countries' administrative procedures and the data required for those procedures add to the complexity, it is important to use the results from reports like these to pinpoint trends of developments and opportunities for sharing best practices.

The current study aims to provide insight precisely in this direction. It will reveal major barriers and risks for harmonization of the European eGovernment landscape, but also drivers and enablers that may be used to address the risks and barriers. Although working with a constrained dataset, the study relies on a multi-method framework that joins different approaches and data sources to provide relevance and scientific soundness.

4.3 Benefits of implementing Once Only

The implementation of the OOP is expected to yield beneficial outcomes for the end user, while at the same time affect digital public services. Moreover, the beneficial outcomes will positively affect the European public administrations. Figure 1 indicates the average expected benefits of the OOP implementation from the responding countries. It shows a very positive picture regarding the benefits of implementing OOP both nationally and cross-border.

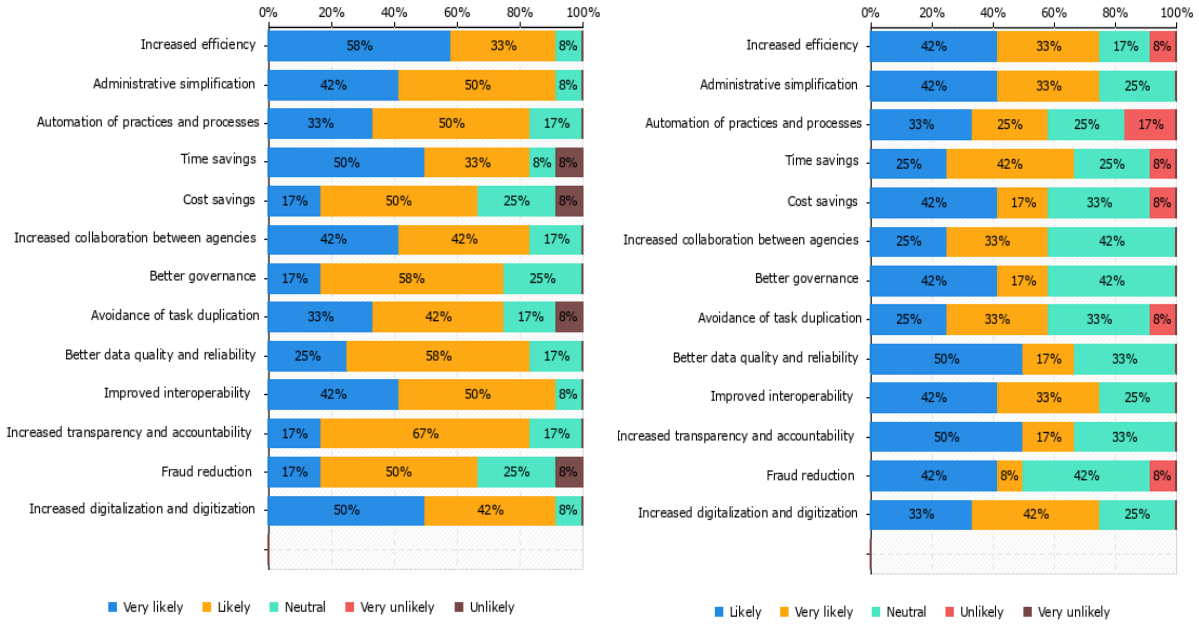

Figure 1: Average expected benefits from OOP implementation: a) national; b) cross-border

In most cases, the responding countries expect the beneficial outcomes to be more likely on a national level compared to its cross-border equivalent. In several cases, there is even the impression that the

OOP implementation will not have any effect on the given indicator. Neutrality of opinion[1] is much present when it comes to cross-border OOP implementation, skewing the distribution of the data for the rest of the indicators. However, some interesting observations can be made regarding several of the indicators for the two cases (national vs. cross-border): Fraud reduction and Transparency & accountability are estimated to be affected much more in the case of cross-border implementation, similar to Cost savings and Data quality. This is somewhat expected, as the requirement by the SDGR especially affects the requirements for data exchange between countries' public administration, but is not defining how SDGR principles will be enshrined in the national laws. Reduced fraud is also directly correlated to the increased transparency and accountability. On the other hand, Collaboration between agencies and Time savings is expected to bring more benefit at the national level. This is also natural to expect, as the frequency of interactions and entity requests to the public administrations is much higher for a national context.

From a national perspective, four factors are equally identified as the most likely benefits: Administrative simplification, Increased digitalization, Increased efficiency, and Improved interoperability. More than 90% of the countries find them as a likely or very likely national outcome of OOP implementation. Only four of the indicators received an expectation for being unlikely to improve in a national context.

Similarly, the overall picture of perceived benefits of OOP implementation in a cross-border context shows very high expectancy. Thus, 50 percent or more of the respondents consider all of the factors to be likely or very likely. Some reach even more than 70 percent likelihood. Only six of the indicators received an expectation for being unlikely to improve in a cross-border context.

In addition to showing the benefits of OOP implementation, Figure 1 also demonstrates the level of certainty in expressing the overall attitude towards the OOP benefits in national and cross-border. Thus, it is evident that the assessment for a national context are not only more positive overall, but are also stated with greater certainty.

In general, responses for considering a certain benefit to be "Unlikely" are mainly expressed by only one respondent for a given indicator. Moreover, no country expressed opinion for a "Very unlikely" beneficial outcome. Compared to the results from the first phase of the WP1 survey, which were also considered very positive, there is a noticeable positive trend for perceived improvements with the implementation of the OOP technical system by all European countries. Considering the fact that the implementation and the proper functioning of the SDG depends largely on the established trust among the public services across all European countries, the results of the survey can serve as an argument for moving towards the desirable direction of meeting the 2023 target.

4.4 Barriers to the Once Only Principle

As described in the section above, the respondents' reviews of the likelihood of various benefits of the OOP implementations are very positive both nationally and in a cross-border context. This begs the question why actual implementation levels are still relatively low? Evaluating perceived barriers that impede the European OOP implementation for the respective national governments might provide some understanding of the current implementation levels.

Figure 2 shows the respondents' view on the barriers to national and cross-border implementation of the OOP technical system and data strategy. Some concrete barriers have been listed (as provided by the respondents) in Table 1. The figure clearly demonstrates a need for addressing the barriers of all types, with lesser or greater criticality and need for immediate action. The highest criticality is assigned to the Human factor, deemed Critical to address immediately by as much as 40% of the responding

[1] Neutrality of opinion means that respondents have not formed an opinion on the benefits from the OOP implementation for the particular indicator

countries. It is followed by the Legal (31%) and Organizational barriers (33%). The legal barriers are mainly expressed through the need for integration with the GDPR (data protection), the problem of identity matching, delays in the implementation of the regulatory prescriptions for the OOP system, and the legal certainty of the security measures. The organizational barriers, on the other hand, are seen in the lack of coordination in the implementation of the OOTS, the lack of both organizational and human resources, and the demanding administrative procedures for government bodies. For instance, OOP and data sharing are embedded in the Spanish legislation for the public for several years already. However, data protection is still a major issue than is mainly left for handling by the bigger competent authorities.

Some national laws also overlap in their jurisdiction. Only in around 20% of the cases, Business and Political factors have not been ascribed to be barriers for the OOP implementation. Moreover, neither is seen as critical to the OOP implementation.

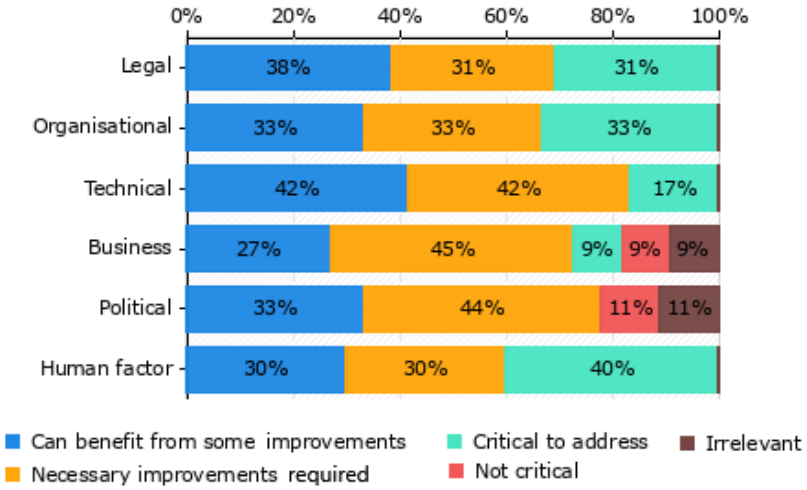

Figure 2: Types of barriers for OOP implementation and level of criticality

Table 1: Description of barriers for OOP implementation, by type[2]

Type of barrier	Description
Legal	1. GDPR (data protection), identity matching 2. The adoption of the implementing regulation for the once-only technical system was delayed by around one year. This is a critical issue, which suggests us to think that the system will not be developed in required timeline (December 2023). 3. Legal certainty of security measures 4. Some national laws overlap in their jurisdiction
Organizational	1. There is no implementation coordination mechanism active yet, and we have issues with available resources at this moment to use and support once-only technical system. 2. Scarce human resources 3. Administrative procedures are too heavy and demanding for government bodies
Technical	1. Lack of standardization 2. Legacy technical resources

[2] The numbering of the barriers has no prioritizing purpose

Type of barrier	Description
	3. Various technical platforms in use (no standardization), old technology, vendor lock
Business	1. Scarce economic resources 2. User involvement in the creation of IT services
Political	1. Poor understanding of the importance of digitization 2. Insufficient number of public servants involved in DSI, fluctuation of employees, lack of IT skills
Human factor	1. Lack of awareness 2. Some barriers are yet to be identified since both the technical system and the implementation strategy are work in progress. Data strategy has also not been launched yet.

However, issues around data protection are not only noticed at a national level. In fact, one of the major challenge of the SDGR procedures themselves is ensuring the legal basis for the transfer of evidence, which may or may not contain personal data. This is precisely what cannot be left to assumption, especially considering the new regulatory steps towards user controlled data flows. The reason for this is that explicit request of the user to transfer any personal data does not automatically entail a consent under the GDPR.

It is important to note here a principal difference between national level once-only legislation and the SDGR: national legislation can directly target specifically identified competent authorities, as they are known and/or identifiable under national law [21]. As administrations may differ widely from one country to another in terms of their designation, competences and capabilities, the SDGR focuses on high level identification of covered procedures, and recommends a choice of competent authorities under a wider set of qualifications covered by Article 3 (4). This implies that a “competent authority” may as well be a private sector entity qualified as a competent authority under the SDGR. This leaves greater possibility for including the private sector in the implementation process, an act that goes in line with the drawbacks put forth by two of the experts interviewed for this report (EBSI / ESSIF and mGov4EU).

Finally, compared to the results from the first phase of the WP1 survey, a clear trend can be noticed on unification of perceived barriers by the countries’ respondents. Considering the rapid advancement of the OOTS implementation and the progress of adopting the SDGR, this development comes as no surprise and can serve as a clear pointer to the common MS problems.

In order to inquire the specificities around the technical barriers for the implementation of the OOTS (which, although not deemed critical, have been claimed as barriers that require most improvements), we asked the respondent about their concerns over specific parts of the OOTS (Figure 3).

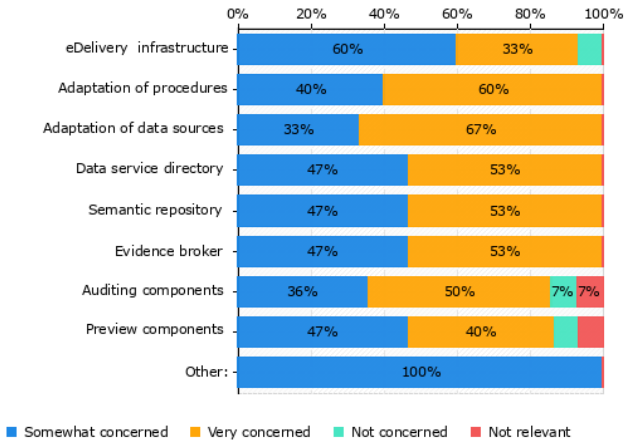

Figure 3: Concern over implementation of the national parts of the OOTS

The results show great concerns over most of the parts and components, the biggest of which are the concern over the adaptation of data sources (shared by 67% of the respondents), as well as the adaption of SDGR procedures to the national context (expressed by 60% of the respondents). The eDelivery infrastructure itself is mainly a moderate concern, while the auditing and preview components invoked various extent of concern – from no concern (in 7% of the cases) to Very big concern, in 40-50% of the countries.

4.5 General attitude towards aspects of OOP

The success of implementing changes in important sectors of a country and across public services depends on the citizens' trust in government and willingness to share data with relevant organizations. Thus, cultural and historical diversity among the European countries both influence the structure of public services and have a major impact on how those are conducted in the different European regions. The correlation between trust in public administrations and digitizing public services can therefore be seen as both a barrier and a driver to implementing national and cross-border public services.

In the survey, we asked respondents to evaluate the general attitude and willingness towards sharing data and towards organizational change in their respective country, for different aspects of OOP. Figure 5 depicts the results of these evaluation, for both public and private organization, as well as for citizens. The figure shows that there is big difference in the inclination toward data sharing and changes in the three cases, with a prevalent qualification of public organizations as being mostly open, as opposed to the private companies' "Very cautious" attitude towards different aspects of the OOP. However, when it comes to sharing personal data with other countries as well as domestic private organizations, most responding countries report on average a very cautious attitude. Only the willingness to share data with public organizations within the country can be interpreted as a more positive and open attitude towards sharing data.

The attitude towards sharing data with public organizations within the country is mostly to very open for about 70% of the countries. However, when considering personal data, only 33% of the countries report a somewhat open attitude when it comes to sharing personal data with public organizations, and 25% for sharing personal data with private organizations. Generally cautious stance exists on the other aspects of OOP implementation as well, although the data sharing aspect is especially standing out in that regard, for both public and private entities.

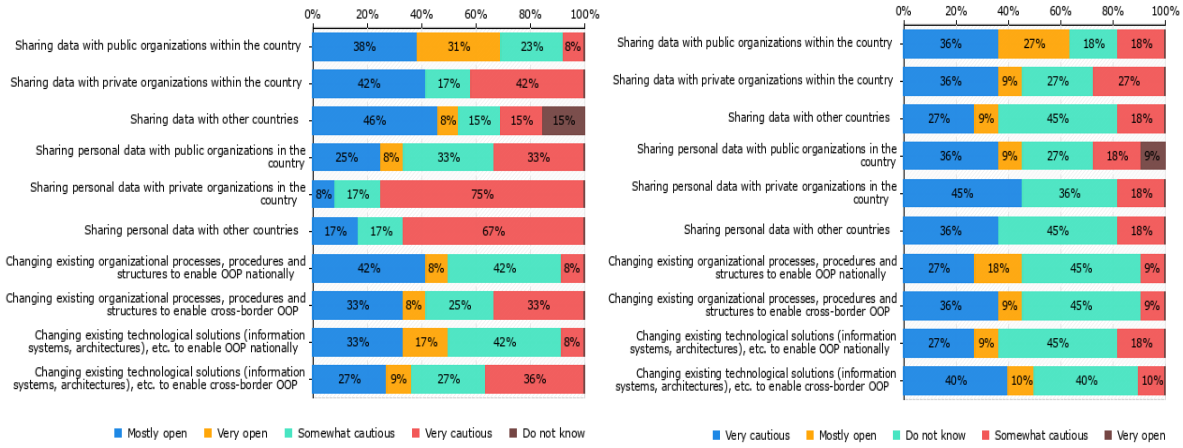

Figure 4: General attitude and willingness towards the shown OOP aspects: a) public, b) private organizations

Although there is a general picture of cautiousness for sharing data and big reluctance towards processes and technological changing (both at a national and cross-border level), compared to the results from the first phase of the WP1, there is a trend of shifting towards more positive attitude on all aspects. We should bear in mind that this also comes with the advancement of the OOP implementations across all countries, which is a sign of positive general change, however slow the progress may seem.

In addition to the willingness towards sharing data, the survey also inquired about the countries' attitude towards changing organizational structures and technological solutions to enable OOP nationally and cross-border. These organizational aspects include processes, procedures and structures whilst the technological solutions refer to information systems, architectures, etc.

Similar to the data sharing case, it can be observed that the corresponding countries are somewhat reluctant to changes, both organizationally and technologically. However, compared to the results obtained from the WP1 survey in the first phase, there is a much more open attitude for change. On the side of the public entities, the openness to changes has increased most for the OOP implementation in a national context, whereas for private entities – in a cross-border context. Furthermore, there seems to be a more reserved attitude for changing technological solutions, although by a small margin. The biggest barrier that can be observed in this context is that the responding countries are reluctant to change their own organizational structures or technical solutions to enable cross-border implementation of the OOTS. More than half report a somewhat to very cautious willingness to change.

From a user-centric perspective, trust in government and thus willingness to share data with public and private organizations tends to be higher in small countries. It is therefore pertinent for the bigger picture to have the citizens' attitudes on the different aspects of the OOP system. Figure 5 shows the results of the survey on the aspects discussed above presented from the point of the citizens.

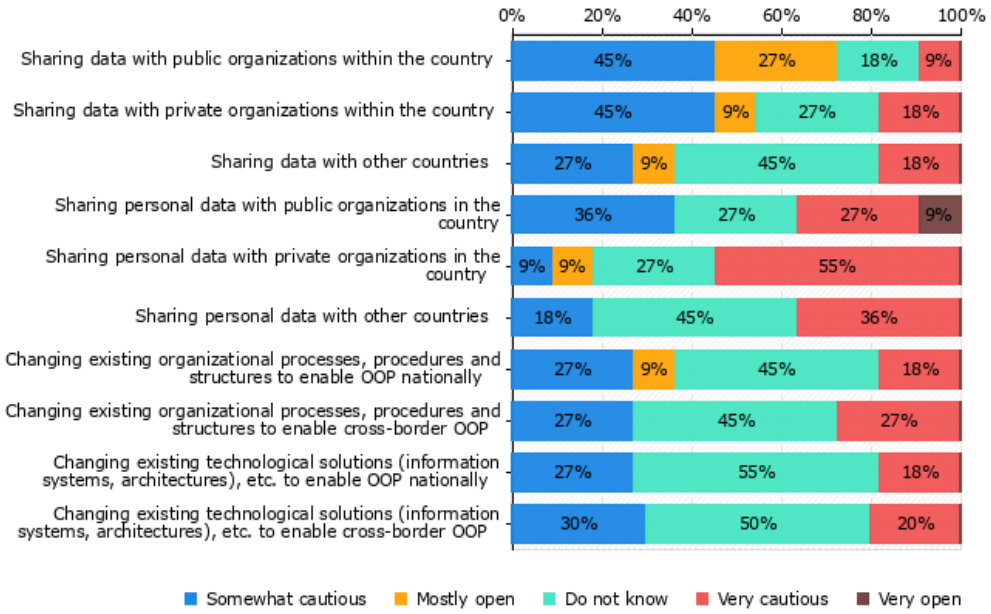

Figure 5: Citizens' attitude and willingness towards the shown OOP aspects

The figure shows similar willingness of citizens to share data with public and private organizations within the country. However, when it comes to sharing personal data, there is a clear difference in the attitude, with much greater readiness to share personal data with public organizations than with private entities. Based on results from other surveys on this particular question, it can be claimed that the reason for this difference in attitude is the greater accountability that public institutions have in this regard. On the other hand, the GDPR brought about changes in this regards, introducing sanctions for private entities should they not comply with regulatory requirements. Thus, the lack of transparency and possibility for redress may be more relevant drivers behind this result.

Interestingly, the citizens' willingness to share data and to accept the organizational and technological changes of the OOP implementation is almost opposite from the one of the public institutions. It is thus clear why respondents stressed the 'Lack of awareness' and 'User involvement' as one of the main Human factors' barrier for the implementation of the OOTS.

From the citizens' perspective, there is almost no distinction between national and cross-border context in the willingness to change existing technological solutions and adapt to new organizational process. In contrast, public and private organizations show diametrically opposite attitudes in this regard, with public entities being more inclined towards the changes on national level, whereas private organizations leaning towards involvement in the changes happening in the cross-border context. These results bear great similarity with those obtained by the WP1 survey in the first phase.

Although it may seem that this analysis represents a negative picture and even the presence of cultural barriers towards OOP implementation, it is important to consider the quality of the feedback. Notably, aside from the incomplete list of European countries represented by this data, there is also skewing of the distribution due to the high uncertainty in the answers (countries who responded with 'Do not know'). However, taking into account additional sources and reports as well, it can be claimed that there is a certain lack of citizens trust in the public administrations and a low willingness to share the data (especially personal data) as a result. This, together with the reluctance to changes that the new regulatory landscape brings, may impose difficulties for the further implementation of the OOP systems and, as a result, on the overall performance of the cross-border public services. This especially holds if considering the low readiness for changes and the openness for data sharing by all three actors: the public and private entities, and the citizens.

4.6 National legislation governing Once Only

The previous section indicated a cautious attitude and relatively low willingness of European countries and their citizens towards sharing data, as well as changing organizational structures and technological solutions. Although we mentioned the cultural diversity as one of the factors, we did not justify our claim with any proof that supports it. We may thus ask: can the willingness to share data or be prone to changes be affected by other means than just by the cultural background? For instance, can citizens' trust in public institutions be affected positively by regulatory means? Or can trust among public administrations from different states improve by legislative means? In this section, we analyze existing regulation at national level to see its effect on the factors related to OOP implementation.

As Figure 6 shows, almost all of the responding countries (94%) have a specific national legislation in place governing the OOP implementation and functioning.

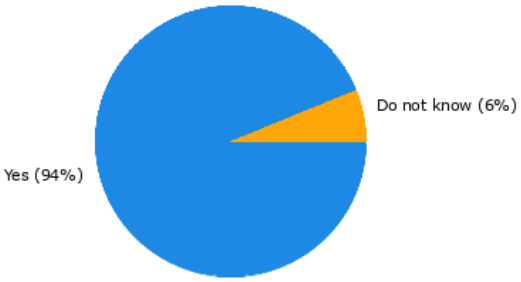

Figure 6: Specific national legislation governing OOP

However, it is important to note that data in Figure 6 refers to legislation that allows or requires a public administration to exchange information in relation to a specific user, directly from a trustworthy source to another public administration. As the political and administrative systems differ across different countries, there may be differences at the procedural preconditions for data exchange under the relevant national legislations. This is out of the scope of this report, but from the contextual remarks made by the respondents for their respective countries, we can observe that there are different legal and regulatory safeguards in place that govern data exchange even for countries that reported partial implementation of the OOP systems. For instance, we often see various types of authorization as a legal precondition for data access at national level (e.g. access to base registries by depending on the type of the private entities and/or the access purpose). This is broadly discussed in the D1.4 report, which hugely complements the current documents with contextual data and more in-depth analysis.

There is one peculiarity about claiming that something is a barrier, or an enabler, for that matter. Namely, it is often the case that the same factor can be both an enabler and a barrier, and this largely depends on the context and even the timing of the analysis. For instance, being a prerequisite for data exchange in the OOP technical system, prior authorization procedures may be perceived as a barrier. However, considering that it provides certain safeguards and facilitates the establishment of trust in the public services, it may as well be seen as an enabler.

Clearly, national law is a complex matter in itself, and putting it in a cross-border context even more so. The responding countries were also asked whether their respective legislation makes a distinction between requests coming from public administrations within the country compared to from other countries. Specifically, whether there would be any part of the law, which would make it impossible or harder to apply the OOP towards requesting data in or from other countries. The answers are presented in Figure 7 and show that the majority of the countries (57%) make no legal distinction

between the national and cross-border data requests, although there is also a significant portion that make such distinction.

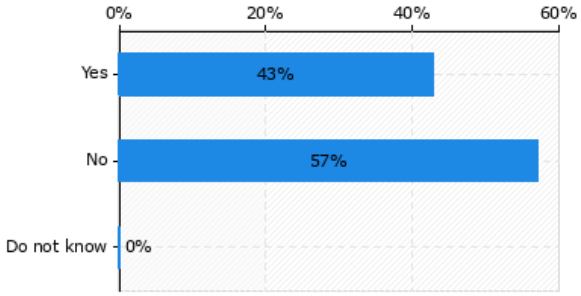

Figure 7: Legal distinction between national and cross-border data requests

To make this distinction possible, but also to analyze the legal means through which OOP implementation is driven at a national level, Figure 8 shows the complementary sources for OOP regulation. The results show that written guidelines and recommendations are the prevalent means that complement the national OOP legislation, although there is similar representation of non-legislative measures and unwritten practices as well. The results for "Other" was used to point out the various legislative references that address OOP implementation at national level. Notably, Spain has developed a separate national legislation act on OOP. Moreover, OOP monitoring is included in main administrative legislation, such as the state administration structure law. OOP and data sharing are embedded in the Spanish legislation for the public sector for almost a year now. Data protection is the main issue that can only be handled by the major competent authorities. The lack of human and technical resources are the main barrier for a full implementation. Similar case is observed with Croatia, with its DSI law. In Belgium, the OOP provisions have been integrated into a separate legislative requirement since 2014[3]. More specifically, the law imposes on the federal authorities (defined in Article 3 of the Law) the obligatory (re)use of unique keys entity identification, and information from the various databases that via the service integrators allows this data to no longer be requested from the data subject(s).

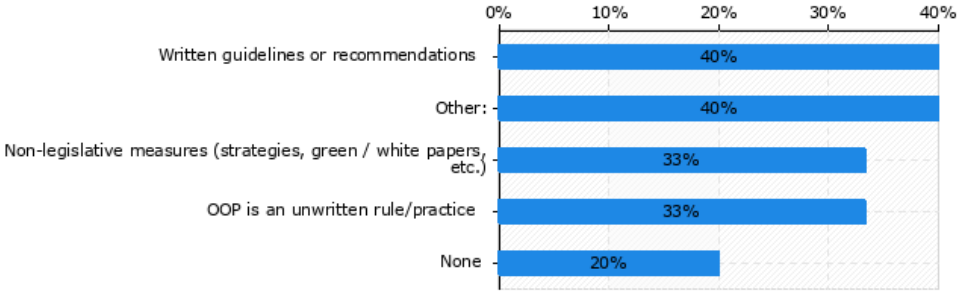

Figure 8: Complementary sources for OOP regulation

Taking into consideration that all countries reported legal barriers among the most challenging to address, it is certain that this the process of addressing this barrier will take longer time and will require additional resources. The fact that the majority of countries report addressing OOP with soft-law measures while also having national legislation in place, shows the need for harmonization of the different national laws in order to enable faster adoption of the SDGR through successful implementation of the OOTS. However, there are also challenges inherent to the regulations

[3] For further information consult https://kafka.be/nl/only-once-wetgeving

themselves, which cannot be addressed only by adapting the national solutions. For instance, the scoping of the data exchanges within specific procedures in the SDGR, the rules for data sharing at a national level (which does have implications on the OOP and the SDGR, but is not addressed by the Regulation), the legal safeguards about reuse of the technical building blocks (catalogued in D1.6), etc. are all challenges that are currently supported only by assumptions for correct use, but are not addressed by the Regulation. Additional analysis in this regard can be made on the interdependencies with the other Regulations (like eIDAS and GDPR), which only adds to the existing complex picture of the legal and regulatory aspect of the eGovernment landscape. Some of these interdependencies will be discussed in the next section, which overview the barriers and drivers introduced by eIDAS, SDGR and the Digital Services Infrastructures.

5 Inventory of risks and barriers

This section discusses the risks and barriers related to the implementation of: the eIDAS, including existing Digital Identity Wallets as a transitional model towards the EU Identity Wallet; the Single Digital Gateway Regulation, and the Digital Services Infrastructures. The specific risks and barriers on the OOP implementation were elaborated in the previous section (see: Barriers to the Once Only).

5.1 eIDAS and trust services risks and barriers

Figure 9 shows the distribution of barriers according to their type and the level of criticality associated with them by the responding countries. While the eIDAS implementation does not encounter highly critical barriers, there is still large space for improvements, especially at a national level. The technical system is already mature enough as to not introduce critical risks, but some improvements are still recommended, more specifically - in regards to identity matching and harmonized data formats. All other factors are to lesser or greater extent present across most of the countries.

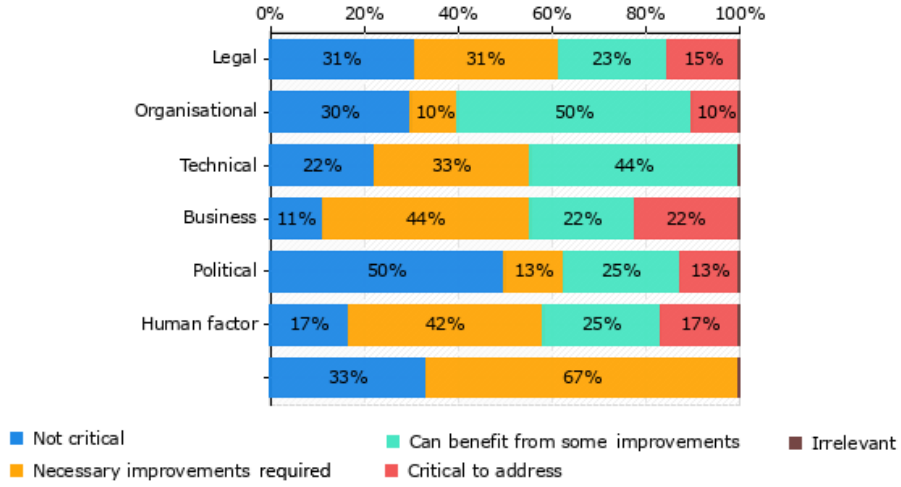

Figure 9: Extent of criticality of the risks and barriers for the eIDAS implementation

While some of the barriers are straightforwardly provided by the respondents and sublimed in Table 2, others are inferred through the data analysis of the DE4A Survey (See Annex) and widely discussed in the D1.2 and D1.4 reports.

Information in the tables showing the barriers (throughout the entire section) represents the direct answers of the respondents, processed for clarity and cleansed for redundant answers. This is done in order to show a directly perceived state as provided by the national representatives, rather than our own interpretation of their meaning. It would allow the reader to also draw own conclusions that may be different from ours. Furthermore, the numbering, i.e., the order of the barriers is not an indicator for prioritization or any type of grading, but merely informs of the overall number of the barriers of a certain barrier type.

Table 2: Inventory of risks and barriers for the implementation of the eIDAS elements

Type of barrier	Description
Legal	1. Hindering regulatory framework (e.g. private SPs cannot access the eIDAS node) 2. Lack of technical standards for interoperability

Type of barrier	Description
	3. Lack of specific national legislation regarding the requirements for the private sector electronic identification providers 4. Regulation requires amendments 5. "According to the current eIDAS regulation countries can choose if they want to notify their eID schemes – this approach is not working as we still have not covered all EU countries." 6. Restrictions on sharing of national identifiers. 7. Lack of knowledge of Regulation by legal experts 8. Inconsistency of the national law with the eIDAS Regulation during first three years of its implementation 9. From eID point of view, the technological development of electronic identity is not followed fast enough by the regulations. Certain changes, due to their nature (rapid development, or technological provision that cannot be standardized, such as the smartphone market) are not covered with the eIDAS implementation acts, so it is difficult to implement them consistently in national law.
Organisational	1. Coordination structure does not fit into business requirements 2. Organizations are not aware of eIDAS regulation 3. Lacking the business model for offering the solution and support for eIDAS authentication to the private sector 4. Relying parties are reluctant to recognize eIDs from other Member States, especially due to difficulties with identity matching 5. Lack of awareness on the use and legal value of trust services 6. Divided competence over the Regulation
Technical	1. The eIDAS node requires specific expertise and effort to be maintained. 2. Identity matching: the current eIDAS does not mandate that countries provide a unique and persistent identifier. The eIDAS data set is too small and insufficient for service providers. 3. Systems often do not accept the use of digital signatures 4. Insufficient interoperability rules for cross-border business eIDs
Business	1. Lack of human Resources 2. Protracted public procurement process 3. Too few attributes available through eIDAS authentication nodes 4. Lacking the business model for offering the solution for eIDAS authentication to the private sector 5. Lack of prioritization of cross-border eGovernment Services
Political	None reported
Human factor	1. Lack of specific expertise 2. IT expert scarcity due to non-competitive payments in the public sector 3. Lack of user awareness on availability and use of eGovernment services by the general public 4. Poor user experience when using cross-border eIDAS authentication 5. Lack of human resources with sufficient technical knowledge on eIDAS.

5.2 Digital Identity Wallets Drivers

As the topic of Digital Identity Wallets is relatively new, and the implementation of the EUDI Wallets is yet to unroll (and formally not yet decided conclusively), this sections inquires only about the drivers that may benefit and facilitate this process. These are enlisted in the table below, whereas the extent to which their exploitation is important in a national and in a cross-border context is shown on Figure 10.

Table 3: Inventory of drivers for the implementation of Digital Identity Wallets

Type of driver	Description
Legal	1. Raising awareness around privacy concerns
Organizational	1. Governance model in place 2. Stakeholder coordination
Technical	1. Security 2. Interoperability
Business	1. Business model (who pays for what ?)
Political	1. Policy choice to allow citizens a stronger role in managing their identity data
Human factor	1. Usability of the solutions 2. Understanding of the solution and digital savviness (e.g. knowing the difference between qualified vs not qualified trust service)

From Figure 10, it can be seen that the Technical, Business and Human factors are considered to be critical for exploitation to drive the changes for DIW implementations in both national and cross-border context. Following the reasoning from Table 3, this would imply that ensuring security and interoperability of the technical system, as well as transparency as to who decides on and benefits from the business models integrating the DIW solutions would be decisive factor in the adoption and the take up of the digital services.

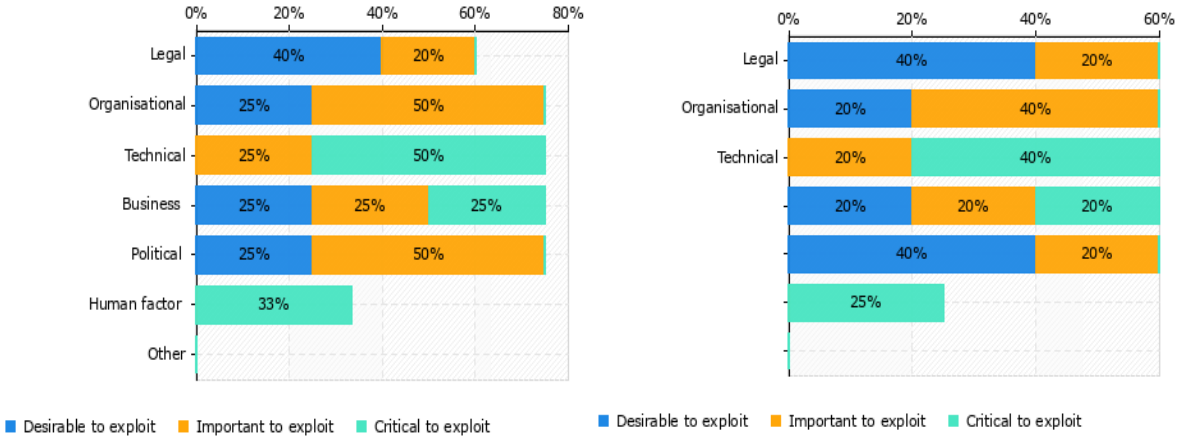

Figure 10: Importance for exploiting the types of drivers for the implementation of Digital Identity Wallets: a) for national purposes; b) for cross-border purposes

Moreover, equally important would for the users to be well introduced into the potentially new technologies by user-friendly solutions offering and protocols offering the option “Do it the old way”.

All drivers are assigned High level of importance by most of the responding countries, and their significance is almost identical at both national and cross-border level. Interestingly, only the political factor is deemed as somewhat more important for cross-border DIW implementation.

Although in most of the countries, Digital Identity Wallets are in their infant stages, experiences from the implementation of the OOP and the eIDAS already provide a valuable knowledge base on the risks and the drivers the implementation of the DIWs may encounter. Many of the countries do not offer a DIW solution, but most have it envisaged for the upcoming period, preparing the ground as per the Recommendation of the revised eIDAS. For instance, the Spanish law does not support self-sovereign identity means, but it is considered a desirable approach for the future. Spain is already leading many EBSI groups and pilots, along with other blockchain initiatives to develop the potential of this new approach. Similarly, with the introduction of the eID in Liechtenstein, various projects have been implemented that are not common for the other European countries, such as the digital driving license. There is also a proposal for several DIW solutions.

5.3 SDG procedures risks and barriers

In inspecting the barriers on the implementation of the SDG procedures (see Figure 11), we see higher level of criticality for most of the factors, and also compared to the other analyzed topic. It is interesting to observe that these levels are quite comparable with the ones analyzed for the barriers for OOP implementation on Figure 2.

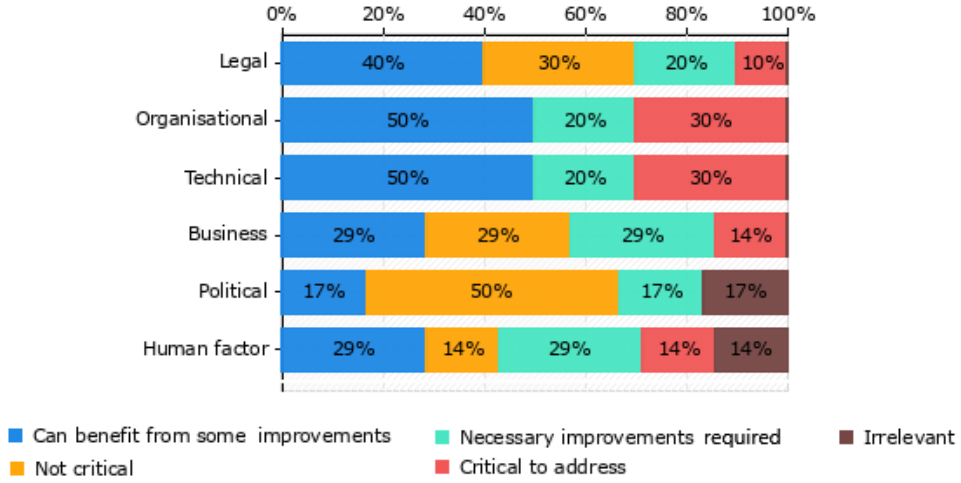

Figure 11: Level of criticality of risks and barriers for the implementation of the SDGR

As the two are highly inter-related, this is of no surprise. However, one difference worth pointing out is the importance given to the Human factor, which in OOP is deemed as critical to address in 40% of the cases, whereas in SDG – in only 14% of the cases. Somewhat smaller differences can also be noted with respect to the Technical barriers (30% in the case of SDG, and 17% for OOP).

The overall picture, clearly, is one of a diverse set of requirements for improvement, which can also be seen from the practical experiences of the responding countries enlisted in Table 4.

Table 4: Inventory of risks and barriers for the implementation of the SDGR

Type of barrier	Description
Legal	1. Problems with OOTS legislative acts. 2. Delay regarding accepting implementation regulation for OOTS leading loss of trust in the national capacities 3. Non-adjusted national legislation

Type of barrier	Description
	4. National language law 5. The Implementing Regulation is still not adopted
Organizational	1. The scope of the procedures is not always clear to public administrations 2. Lack of cooperation between competent authorities 3. No implementation coordination mechanism provided, leading to issues with available resources to use and support the OOTS. 4. OOTS is considered a low priority, 5. Lack of resources is a huge barrier 6. Reluctance to change management 7. National fragmentation
Technical	1. Delay in adopting the implementation act 2. Technical specification documents are not finalized. 3. Problems in reconciling different systems even within the same environment. 4. Not every service is connected to the national OOP infrastructure 5. OOTS is not implemented. Services are not integrated to the desirable extent. 6. Not all authorities are digital-enabled. 7. Lack of technical personal 8. Poor national implementation strategy
Business	1. Low awareness of user-centricity in services 2. Difficulty in contracting proper means for cross-border payment 3. Some OOP aspects constrain the use of digital public services
Political	1. Non-existing digital strategy for public inclusion in the digital transformation
Human factor	1. Low extent of qualified resources for the use of new technologies 2. Lack of human resources 3. Low user awareness and acceptance of new services 4. Scarce technical expertise on SDG

5.4 Digital Service Infrastructures risks and barriers

As part of the DSI barriers, Legal and Human factors the only two deemed critical, and only by a small subset of the responding countries. However, the percent of barriers that invoke Necessary improvements to be made is also relatively high across most of the countries. It is interesting to observe the Political factors, which seems to divide the respondents over its impact on the eIDAS implementation, with half of the barriers being denoted as Political "asking for" necessary improvement in that regards, and half considering it as 'Not critical'.

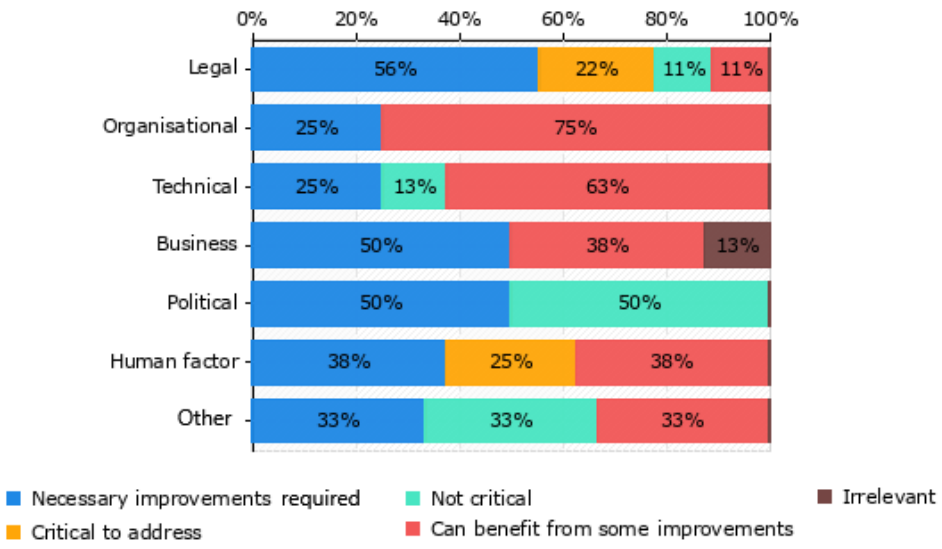

Figure 12: Level of criticality of risks and barriers for the implementation of the Digital Service Infrastructures

Table 5 catalogues the particular drivers, described per type and in the form in which they were provided by the respondents. As explained previously, the responses were processed for consistency and cleansed for redundancy. Although the Legal barriers are most numerous, a huge interdependence between all factors can be noticed, making the analysis that more difficult, as any recommendation in the direction of addressing one barrier will have impact on another. Moreover, what is considered to be a barrier in one context may even be an enabler in another. For instance, legislation that provides safeguards in one context may be an encumbering requirement in another.

Table 5. Inventory of risks and barriers for the implementation of Digital Service Infrastructures

Type of barrier	Description
Legal	1. Impossible to follow what is allowed to be exchanged from what is actually being exchanged as information, 2. Improper implementation of Data Protection Law 3. Lack of legislation to enable data sharing between agencies 4. Lack of technical specifications crystallized in laws. 5. Blockchain cannot be used for electronic identity means 6. Constraints with the location of data and use of cloud services related to the application of the GDPR with regard to the international transfer of personal data 7. Poor implementation of the eIDAS regulation 8. Some national laws overlap in their jurisdiction
Organizational	1. Need for more central management of DSIs 2. Lack of incentives for data exchanges 3. Complex bureaucratic procedures required for exchanging data 4. Lack of resources on the side of public services 5. Not all authorities are digitally-enabled 6. Lack of resources in general 7. Administrative procedures are too heavy and demanding for Government bodies
Technical	1. DSIs need common framework 2. Lack of legacy infrastructures

Type of barrier	Description
	3. Not all authorities are digital-enabled 4. Lack of interoperability, cross-border and cross-domain 5. Lack of standardization, old technology, vendor lock
Business	1. Consolidated business models in the public sector hinders wider data exchanges / Data protectionism. 2. Old business models for public services constraining the use of digital media; 3. Lack of resources 4. Lack of user involvement in the (co)creation of IT services
Political	1. Lack of collaboration at a national level 2. Lack of campaigns to improve the use of digital services by citizens on understanding of the importance of digitalization
Human factor	1. Lack of interest for available e-services and its use 2. Lack of qualified resources for the use of new technologies 3. Poor digital literacy 4. Lack of resources 5. Insufficient number of public servants involved in DSI, fluctuation of employees, lack of IT skills

Clearly, the perception of what represents a barrier differs among different actors as well. Citizens and public sector do not perceive the same benefits from the DSIs, as they do not share similar needs in relation to the DSIs. This is also culturally conditioned and varies greatly from one state to another, which makes the data inconsistent over a single parameter. For instance, in Sweden, DIGG is responsible to gather common barriers from different organizations and present the ideas in Swedish language. For that, the development of a framework and technical specifications for the national eDelivery platform was needed, which benefited to a great extent from the EU base for a standardized implementation. Having a tradition of decentralized management, Sweden has been encountering more problems from an organizational nature and has worked towards improved coordination at national level. On the other hand, Spain is highly active in cross-border initiatives, notably on blockchain, but due to more problems related to national users' need, it considers cross-border implementation as a non-priority.

To conclude, a more granular and careful analysis on the barriers is needed to draw any meaningful conclusion.

6 Discussion

In the previous chapters, various risks and barriers on national and cross-border digitized services have been identified. Furthermore, each barrier has been classified on the basis of its significance as a factor towards inhibiting or driving OOP changes. This analysis, although based on incomplete datasets, integrate the know-how of various experts and draw from different data and information sources to justify the overall methodological framework. As such, it provides insights and draws focus on the most pressing and current issues.

The risks and barriers have been identified for every aspect prescribed by the conceptual framework: Legal, Organizational, Technical, Business, Political and Human. Furthermore, all these factors have been separately mapped and discussed for each of the areas of interest covered by the DE4A Survey: eIDAS, EU Digital Identity Wallets, OOP implementation, SDGR and Digital Service Infrastructures. Figure 13 sums this assertion and provides further insights into the distribution of the barriers per topic and per type. As Digital Identity Wallets have been analyzed mainly from the point of view of their drivers and enablers, DIW is not part of the figure. Interestingly, we see a somewhat uniform distribution of barrier per topic, with OOP itself being the least "criticized". This is to some extent expected, as there is high interdependence between all topics, with OOP implementation being to large extent the result of their successful harmonization across European countries.

The distribution per barrier type shows that Organizational and Legal barriers are the most prevalent, amounting for almost half of the respondents' inputs. They are followed by Human factors, which, although not prevalent by quantity, were deemed as the most critical factor to address over all discussed topics. Moreover, they were also marked as the critical driver to exploit in the context of Digital Identity Wallets (see Section 5.2). Needless to say, the human factor is highly intertwined with all other barriers, as humans are at the core of all systems and services, driving the digital transformation and the willingness to adopt the changes. Therefore, addressing any of the barriers entails working towards addressing the human factors as well.

Finally, as it was also discussed in the analysis of each of the barriers in the previous sections, the Political factor is considered to be least impactful in terms of presenting a barrier. However, this does not imply that it is not a critical element of the set of enablers and drivers. As we have seen with the highly federated states, it is precisely this factor can make huge difference in both implementation and adoption of digital services.

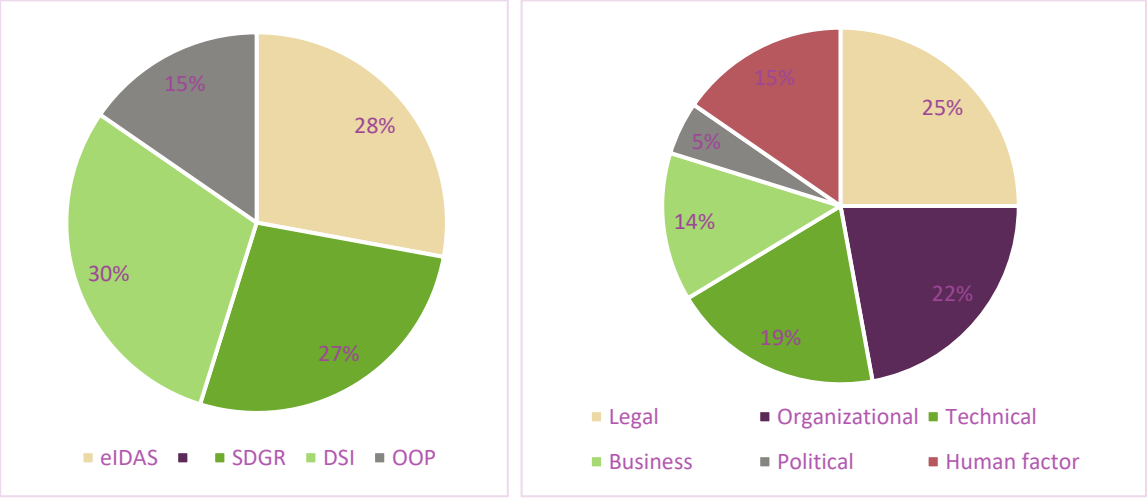

Figure 13: Comparison chart: a) Barriers per topic; b) Barriers per type

Even though the analysis presented here is mainly qualitative, the report provides a solid basis for further investigation of each barrier. Moreover, the results point out to a high number of barriers with defining influence on the progress of the eGovernment digitization initiatives across Europe.

The volume and severity of the identified risks and barriers in each of the four layers of interoperability indicate that there is an absence of an operational interoperability governance structure – i.e. one mandated with monitoring and ensuring interoperability. The number, complexity and criticality of the barriers give reason to evaluate how the development of a Single Digital Market may best be achieved, especially when taking into consideration the documented low implementation levels in the previous reports.

Considering the aforementioned low implementation levels of once only and considering an added complexity of cross-border implementation, the clear favoring of national implementation by public administrations, suggests that any cross-border implementation should build upon national implementation efforts. As such, it may appear that cross-border European services are not the core priority for many governments in Europe, which would call on additional incentives and proper coordination efforts at a regional and European level. However, an alternative explanation may be that cross-border OOP services are not implementable without EU level coordination, which is still to become fully operational under the SDG. In any case, the near future shouls strike a conclusive remark on this issue.

Complemented by the overwhelming reluctance to change organizational structures and the lack of resources of human and technical nature, there is an indication that support is needed to the Member States in handling ongoing, pressing and costly issues.

This can be explained with different reasons: actual cross-border interactions may still be so limited that converting digital infrastructures to meet the needs of the few is still too costly. Furthermore, the need for cross-border services may not be perceived urgent enough to be set as a national priority. Finally, the importance of citizen inclusion and its connection to improving lack of awareness and interest may not be well-understood by the public actors.

The report also indicates that abandoning the traditional bottom up approach is needed however to prevent data and service silos, but also to address domain-specific problems. This, clearly, is not without risk. But not going that way may be the riskier choice, as it may also lead to losing the local support necessary for proper implementation.

The overall impression on the gap between the ambitions laid down in the European initiatives and the actual implementation levels in the Member States furthermore invites many questions. For instance: can the processes of drawing up and negotiating new European initiatives lead to more beneficial initial results through a multi-stakeholder and interdisciplinary approach? As this specific part of the process was out of scope for this study, further research is recommended in order to find ways of bridging that divide, ultimately to the benefit of everyone involved in the processes and those for whom the services are to be developed.

On this basis, the next section provides specific recommendations directed relevant for all stakeholders in the eGovernment landscape.

7 Recommendations

Based on the discussion provided in the previous section, and the results presented in the study, this sections presents a sublimed list of recommendations for enablers in reference to each type of barrier detected through the data analysis. It may be a worth exercise to catalogue these enablers in view of the types of eGovernment stakeholders, so as to produce a narrowly directed set of policy recommendations. However, this is not in the scope of this report.

Table 6: Recommendation for enablers per barrier type

Name of the Factor	Recommendation for Enablers
Legal	1. Alignment between policy and practice is needed, especially in terms of implementation timelines of the efforts 2. Incremental amendments to national laws should follow the state of technological advancement, independent on the pace of revising Union Laws 3. Detect all interdependencies between SDGR, GDPR, eIDAS to enable better coordination through federated registry of authorities' competences: - Increased focus is required on legal policies to accept digital evidences - Data protection in the SDGR should be guaranteed by legal means - semantic standardization of user consent, technical solution to transfer the (proof of) consent should be based in line with the eIDAS - Ensure legal basis for reuse of consent implemented by development of standardized notification mechanisms with the option for revocation of the given user consent 4. Ensure legal basis (for providing accountability means) and easy access for users to revoke consent. 5. Provide means for implementation of standardized evidence
Organizational	1. Increase accountability and transparency through (self)monitoring and (self)evaluation mechanisms, including auditability of the data exchanges This should also be available (preferably via interoperable interface) to other MSs and bootstrap collaboration on these tasks. 2. Establish coordination networks of initiatives with consistent objectives - based on inter-dependencies - to prevent information and resource silos 3. Interoperability frameworks should ensure productive feedback that allows revision of the interoperability principles and requirements for the future efforts 4. Reconsider the scope of implementation to minimize operational risks and ensure effective change-management 5. Cross-border digitization should build upon national digitalization efforts 6. Enable implementation of interrupted procedure 7. Establish protocols for ensuring legal value of data retrieved from authoritative data sources 8. Reduce cross border transactional fees for public data 9. Design and implement governance structures that can support lifecycle management of required components and services, including more granular specifications for interfaces and processes.

Name of the Factor	Recommendation for Enablers
	10. Determine and implement measures and standards to manage and monitor data quality. 11. Alignment of policies and deployment of frameworks like EIF with focus on cross border interoperability. 12. Encourage reuse of digital infrastructures to reduce costs for implementation and operations 13. Establish open data repositories with documented good practices, lessons learned and recommendations that explicate and mitigate the different barriers.
Technical	1. Ensure reuse and implementation of fundamental building blocks. 2. Improve resilience and increase availability of ICT resources 3. Increased focus on use of building blocks and standards and deployment of generic infrastructure services under a cross-sector governance, such as the eIDAS eID network. 4. Implementation of standardized generic cross border infrastructure services such as eID, eSignature and data sharing. Interconnection of national infrastructures with standard interfaces to enable cross border transactions for national systems. The effort to interconnect national solutions and infrastructures may be more or less complex depending on the legacy systems architectures. 5. Develop architectures with clear division of responsibility and user-friendly interfaces. 6. Establish a transitional model for revising national eID means that support current mobile solutions, but complies with the eIDAS revision as well 7. System to match criteria and evidences (Evidence Broker) and Data Services to data sources (Data Service Directory) 8. Agreement on a common data format for structured and non-structured documents. 9. Use of canonical forms or common data models based on European Core Vocabularies 10. Mapping between sectorial ontologies and domain-agnostic vocabularies should be enabled 11. The data request should contain sufficient verified information to match the citizen identity (presumably based on the eIDAS authentication) to facilitate “real-time” identity matching with the data providing authority registered identity for the specific user. This could include extension of the eIDAS attributes and other verifiable information attributes. 12. Implement functional and available payment solutions
Business	1. Any digitization initiative should strive for a positive return on investment 2. Inclusion of the private sector in both national and cross-border OOP implementation and developments 3. Investments in new technology and infrastructure, including portal solutions for public service provision, may actually lower operational costs and the resources for non-digital (physical) support

Name of the Factor	Recommendation for Enablers
	4. Crafting strategies for change management that do not interrupt current business models 5. Determine perceived risks that inhibit the process of digital transformation and cause isolated design of proprietary digital solutions
Political	1. Shape new models for public services without constraining the use of digital public services 2. Enable multi-stakeholder dialogue that is timely and inclusive 3. Encourage active cooperation in the digital transformation between all levels of government. Promote and adopt policies supporting this process at a transnational level
Human factor	1. Establish coherent dissemination efforts to raise user awareness on available e-services in order to improve service adoption 2. Increase the trust between public and private sector, setting both national and cross-border digitalization issues as a common interest and goal 3. Organize trainings and campaigns to inform and support the digital readiness of administrative workers 4. Establish incentive schemes within organizations to ensure that digital expertise is not a scarce resource 5. Provide guidelines for building human capital as an investment in the digital future

A similar note can be made as it was noted for the barriers: the high context-dependency of these matters and the inter-twined nature of the different types of enablers prohibit any general conclusions and recommendations as to how to apply a specific enabler for addressing a specific barrier. Such deliberations can only be made for a narrowly scoped problem, with clear interdependencies established among the relevant actors. Neither the data nor the scope of this report allows for such exercise.

8 Conclusions

In this study, the European eGovernment landscape was analysed with the objective to extract legal, technical, organizational, business, political and barriers that stem from human factor. The approach also accounted for the contextual and cultural traits of the countries that provided feedback to an extensive survey on the implementation of national and cross-border digital public services.

The identification and description of the risks and barriers was based on a conceptual framework designed specifically for this report, and implemented through the empirical research based on three data sources: a survey among the Chief Information Officers of the EU and EFTA Member States, a thorough desk research on relevant academic efforts, European projects and initiatives and current regulatory efforts, and semi structured experts' interviews with internal (DE4A) and external experts on the topics of interest.

By applying the conceptual framework as a guiding methodology, detected and described were 104 risks and barriers across the six conceptual layers: legal, technical, organizations, business, political and human factor. For each risk and barrier, a list of enablers in the form of policy recommendation was complied, amounting for 44 enablers directed at the various eGovernment stakeholder.

The study found that the prevalent types of barriers that countries face in the implementation of public services are of Legal and Organizational nature, whereas the most critical to address is the Human factor. Lack of resources and lack of expertise are the most painful points from organizational point of view, while non-harmonized law – from a legal point of view. Lack of awareness on availability of services and reluctance to change and adoption are the most critical problems that require immediate action.

Although each risk or barrier may be categorised in some of the six conceptual layers, all factors are intertwined and have implications on the others. This adds further complexity to the effort to output a meaningful recommendation targeted at addressing a particular risks or barriers. At the same time, what is risk in one context, may appear as an enabler in another context.

Finally, it is worth noting that the SDGR is a milestone and an enabler in and of itself. As an attempt to create a legal framework for cross-border once-only functionality, it provides a successful bootstrap for the implementation of the technical systems relevant for OOP and eIDAS, while challenging the GDPR in contexts not assumed by the regulation. This creates an atmosphere for a positive change that goes in the direction of providing user-centricity and technological innovation.

References

[1] "eGovernment Benchmark 2022 | Shaping Europe's digital future." https://digital-strategy.ec.europa.eu/en/library/egovernment-benchmark-2022 (accessed Sep. 12, 2022).

[2] "Digital Economy and Society Index (DESI) 2022 | Shaping Europe's digital future." https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022 (accessed Sep. 12, 2022).

[3] "Ministerial Declaration on eGovernment - the Tallinn Declaration | Shaping Europe's digital future." https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration (accessed Sep. 17, 2022).

[4] X. Albouy and M. Richter, "Report on the monitoring of the Berlin Declaration." Directorate General for Informatics, May 2022. [Online]. Available: https://www.numerique.gouv.fr/uploads/20220506_Berlin_Declaration_monitoring_report_2022.pdf

[5] J. R. Gil-García and T. A. Pardo, "E-government success factors: Mapping practical tools to theoretical foundations," *Government Information Quarterly*, vol. 22, no. 2, pp. 187–216, Jan. 2005, doi: 10.1016/j.giq.2005.02.001.

[6] P. Germanakos, E. Christodoulou, and G. Samaras, "A European Perspective of E-Government Presence – Where Do We Stand? The EU-10 Case," in *Electronic Government*, Berlin, Heidelberg, 2007, pp. 436–447. doi: 10.1007/978-3-540-74444-3_37.

[7] A. Savoldelli, C. Codagnone, and G. Misuraca, "Understanding the e-government paradox: Learning from literature and practice on barriers to adoption," *Government Information Quarterly*, vol. 31, pp. S63–S71, Jun. 2014, doi: 10.1016/j.giq.2014.01.008.

[8] M. Gasco, M. Cucciniello, G. Nasi, and Q. Yuan, "Determinants and barriers of e-procurement: A European comparison of public sector experiences", Accessed: Sep. 17, 2022. [Online]. Available: https://core.ac.uk/display/301374426

[9] "EU-wide digital Once-Only Principle for citizens and businesses - Policy options and their impacts | Shaping Europe's digital future." https://digital-strategy.ec.europa.eu/en/library/eu-wide-digital-once-only-principle-citizens-and-businesses-policy-options-and-their-impacts (accessed Sep. 16, 2022).

[10] P. Dunleavy, H. Margetts, S. Bastow, and J. Tinkler, "New Public Management Is Dead—Long Live Digital-Era Governance," *Journal of Public Administration Research and Theory*, vol. 16, no. 3, pp. 467–494, Jul. 2006, doi: 10.1093/jopart/mui057.

[11] H. De Vries, V. Bekkers, and L. Tummers, "Innovation in the Public Sector: A Systematic Review and Future Research Agenda," *Public Administration*, vol. 94, no. 1, pp. 146–166, 2016, doi: 10.1111/padm.12209.

[12] "The ubiquitous digital single market | Fact Sheets on the European Union | European Parliament." https://www.europarl.europa.eu/factsheets/en/sheet/43/the-ubiquitous-digital-single-market (accessed Sep. 17, 2022).

[13] A. Mocan, F. M. Facca, N. Loutas, V. Peristeras, S. K. Goudos, and K. Tarabanis, "Solving Semantic Interoperability Conflicts in Cross-Border E-Government Services," *Semantic Services, Interoperability and Web Applications: Emerging Concepts*, 2011. https://www.igi-global.com/chapter/solving-semantic-interoperability-conflicts-cross/www.igi-global.com/chapter/solving-semantic-interoperability-conflicts-cross/55039 (accessed Sep. 16, 2022).

[14] A. D. GANCK, "The New European Interoperability Framework," *ISA² - European Commission*, Feb. 16, 2017. http://webserver:8080/isa2/eif_en (accessed Sep. 16, 2022).

[15] M. A. Wimmer, A. C. Neuroni, and J. T. Frecè, "Approaches to Good Data Governance in Support of Public Sector Transformation Through Once-Only," in *Electronic Government*, Cham, 2020, pp. 210–222. doi: 10.1007/978-3-030-57599-1_16.

[16] Danish Technological Institute, Directorate-General for the Information Society and Media (European Commission) Now known as, and EY, *Study on eGovernment and the reduction of administrative burden :final report*. LU: Publications Office of the European Union, 2014. Accessed: Sep. 16, 2022. [Online]. Available: https://data.europa.eu/doi/10.2759/42896

[17] C. Merlin-Brogniart *et al.*, "Social innovation and public service: A literature review of multi-actor collaborative approaches in five European countries," *Technological Forecasting and Social Change*, vol. 182, p. 121826, Sep. 2022, doi: 10.1016/j.techfore.2022.121826.

[18] L. F. Luna-Reyes and J. R. Gil-Garcia, "Using institutional theory and dynamic simulation to understand complex e-Government phenomena," *Government Information Quarterly*, vol. 28, no. 3, pp. 329–345, Jul. 2011, doi: 10.1016/j.giq.2010.08.007.

[19] L. Rodríguez Domínguez, I. M. García Sánchez, and I. Gallego Álvarez, "Determining Factors of E-government Development: A Worldwide National Approach," *International Public Management Journal*, vol. 14, no. 2, pp. 218–248, Apr. 2011, doi: 10.1080/10967494.2011.597152.

[20] "Digital Agenda for Europe | Fact Sheets on the European Union | European Parliament." https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe (accessed Sep. 17, 2022).

[21] H. Graux, "The Single Digital Gateway Regulation as an Enabler and Constraint of Once-Only in Europe," in *The Once-Only Principle: The TOOP Project*, R. Krimmer, A. Prentza, and S. Mamrot, Eds. Cham: Springer International Publishing, 2021, pp. 83–103. doi: 10.1007/978-3-030-79851-2_5.

Annexes

Annex: DE4A Survey

Digital Europe for All (DE4A) survey

Purpose of the survey and data protection

Dear member state representative,

On January 1st 2020, the EU member state-driven project Digital Europe for All (DE4A) was launched. DE4A is dedicated to creating an open and comprehensive environment and platform to support public administrations in delivering secure, high quality and fully online cross-border procedures for citizens and businesses. In addition, it will provide insights into the barriers to cross-border interoperability and the enablers for overcoming them. You can read more about the project on the project website, https://www.de4a.eu/.

The survey that we kindly ask you to fill in is a second phase of the data gathering process within the project that takes stock of the deployment of cross-border services. The results and analysis of the first phase of data gathering can be found here, under D1.x deliverables.

We will use the data collected in the second phase to analyze the implementation of specific eGovernment action points in the member states and to get insight into the progress of implementing the technical architecture and the eGovernment environment since the previous stock-taking. The derived insights and good practices will serve as practical guidelines for the development and deployment of digital public services for other EU member states, as well for self-evaluation (together with own experience) of the DE4A architecture development.

The survey consists of several blocks: (1) eIDAS National ID schemes, (2) eIDAS Nodes and trust services, (3) (European) Digital Identity Wallets, (4) Single Digital Gateway Regulation: Life Events, (5) Digital Service Infrastructures, (6) Once-Only Principle and Data strategy. Each of them aims to gather insights into the current state, the implementation process, barriers and enablers, which are to be compiled into separate reports on the elaborated topics.

We kindly ask you to provide your feedback on the current status of eGovernment in your country for each of the blocks mentioned above. With the data collected in this phase, we will compile detailed aggregated reports depicting the overall eGovernment landscape of the EU member states. We encourage you to make use of the comment boxes at the end of every subchapter of the survey in order to indicate legal, technical, or other particularities relevant for understanding the national context.

Please note that the responses obtained through the survey will not considered as the official positions of the EU Member States, and that data gathered will mainly serve to support qualitative analysis of the EU governance landscape.

No individual survey will be published in its entirety, and in case an individual response is found useful for publication, it may only be done through a consent by the responder.

Data protection statement

This survey is performed in the frame of the Digital Europe for All Project (DE4A - https://www.de4a.eu/), which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 870635.

Please note that your participation in this survey implies processing of your personal data. Personal data will be processed in compliance with the Regulation (EU) n° 2016/679 on the processing of personal data (the GDPR). The input you provide will only be shared outside of the DE4A consortium in the form of aggregated data. Within the DE4A consortium, we will process your data in order to analyse your answers as foreseen in accordance with the grant agreement, on the basis of our public interest tasks. For further information or to exercise your rights, you may contact our project DPO via privacy@de4a.eu. These rights include requesting copies, correction, or deletion of your personal data, or restricting/objecting to further processing (all within the constraints of the grant agreement). You have the right to lodge a complaint with the competent data protection authority. Do you give consent to processing the information for the purposes of this analysis under the above condition?

- ○ Yes
- ○ No

Member State Information

Please state the name of the country you are representing: _____

eIDAS: National eID-schemes

This part of the questionnaire takes stock of the implementation of national eID scheme under eIDAS Regulation (EU) No 910/2014. To fill it in, you can also consult the available information on your national eID scheme at the eID User Community.

1. Please insert below the required information regarding the status of your national eID scheme(s).

	Pre-notified	Notified	Peer reviewed
Number of eID schemes			

Remarks: _____

	Level of assurance			
	Low	Moderate	High	Not relevant / Do not know
Number of **eID schemes** with the shown level of assurance				

Remarks: _____

	Level of implementation			
	Necessary national legislation adopted	Implemented for national use only	Implemented for cross-border use	Not relevant / Do not know
Number of **notified eID** schemes with the shown level of implementation				

Remarks: _____

	Official issuer			
	Public entity	Private entity	Public-private partnership	Other
Number of eID schemes whose official issuer is:				

Remarks: _____

2. The eID scheme(s) grant(s) access to the following services (please specify the concrete sectorial services):

☐ National public services
☐ Public services by regional / local authorities
☐ Non-governmental services
☐ Private entities
☐ Do not know
☐ Other: _____

3. Please indicate possession rate for all of the notified eID schemes. (*Possessions rate is the ratio of total number of eID holders to total number of inhabitants expressed as a percentage (citizens + foreign residents).*

eID scheme (1) _____

eID scheme (2) _____
eID scheme (3) _____
eID scheme (4) _____
eID scheme (5) _____
eID scheme (6) _____

4. Please, if available indicate the activation rate for all of the notified eID schemes where applicable. (*Activation rate is the ratio of activated eIDs to the total number of eIDs expressed as a percentage.)*

eID scheme (1) _____
eID scheme (2) _____
eID scheme (3) _____
eID scheme (4) _____
eID scheme (5) _____
eID scheme (6) _____

5. Please indicate the use rate for the notified eID schemes (for cross-border use and, where available, for domestic use). (*Use rate is the ratio of eIDs which have been used at least once to access a public service to the total number of eIDs expressed as a percentage.*)

eID schemes	Use rate	
	Domestic use	Cross-border use
eID scheme (1)		
eID scheme (2)		
eID scheme (3)		
eID scheme (4)		
eID scheme (5)		
eID scheme (6)		

6. Please provide the following information, if available. If not available, mark N/A:

- Number of citizens issued with notified eID-s: _____
- Number of businesses issued with notified eID-s: _____
- Number of businesses actively using notified eID-s: _____
- Number of national online service providers accepting notified eID-s: _____
- Number of online transactions by notified eID-s (total and cross-border):
  Total: _____ Cross-border: _____

7. If there are any documented good practice experiences related to the implementation of eIDAS in your country, please provide a link/reference to the document(s).

_____
_____

8. Please provide additional information which, in your opinion, is important for the understanding of your country's context regarding the topics elaborated in this subchapter.

_____
_____
_____.

This part of the questionnaire takes stock of the implementation of national eID scheme under eIDAS Regulation (EU) No 910/2014.

eIDAS: eIDAS node and trust services

1. State the version of the eIDAS Node proxy and/or the profile supported:

_____
_____
_____.

2. Does your eIDAS-node support using your national eID(s) abroad?

○ Do not know

○ Yes

○ No (if known, please specify expected date of production): _____

If Yes, please respond to the following question:

2) As a **Sending** Member State, which countries is your eIDAS Node interoperable with to provide cross-border authentication of your national eID(s)?*

_____

3. Does your eIDAS-node support the use of foreign eIDs for services in your country?

○ Do not know

○ Yes

○ No (if known, please specify expected date of production): _____

If Yes, please respond to the following questions:

3a) How is the use of foreign eIDs enabled?

☐ Allowed only for identification and authentication in public services
☐ Possible for private sector services wihtout restriction
☐ Possible for private sector services with fee, legal or other restriction
☐ Other: _____

*3b) As a **Receiving** Member State, which countries is your eIDAS Node interoperable with to send authentication requests of foreign eIDs?*

_____

5. Please identify (mark with ***X*** the appropriate field) the advancement level of the following means/services in your country:

	Do not know	Not implemented	Necessary (national) legislative procedures adopted	Implemented for national use	Implemented for cross-border use
Electronic signature					
Advanced electronic signature					
Qualified electronic signature					
Qualified certificate for electronic signature					
Electronic seal					
Advanced electronic seal					
Qualified electronic seal					
Electronic timestamp					
Qualified electronic timestamp					
Electronic registered delivery services					
Qualified electronic registered delivery services					
Certificate for website authentication					
Qualified certificate for website authentication					
Electronic ledgers					
Qualified electronic ledgers (if available)					

6. Is there any framework or a mechanism to monitor the implementation of the Regulation in your country?

○ Yes

○ No

○ Do not know

7) **If Yes**, state the purpose of the implementation, i.e. the functionality of the monitoring mechanism at a national level. Check all that applies.*

☐ To ensure implementation of the necessary changes to the relevant national systems
☐ To overview the extent to which the necessary changes have been implemented in line with the adopted measures
☐ To check whether the necessary changes to the compliance obligations by the regulated entities have been adhered to
☐ Other: _____

7. Indicate the types of barriers that the implementation of the eIDAS elements (nodes, schemes, trust services) has encountered in your country (See the provided examples below):

Legal	***Inconsistency with current legislation, hindering regulatory frameworks, inter-dependence with other regulatory acts or codes of conduct***
Organizational	***Weak or inconsistent management practices, lack of common language among organisational entities***
Technical	***Underdeveloped systems infrastructures, expert scarcity, hindering innovation***
Business	***Market disruptions, lack of market opportunities, closed business pathways***
Political	***Lack of state involvement, political frictions among state players, general political turbulences***
Human factor	***Lack of user awareness, lack of personnel training, expert reluctance to involvements***

(a) Legal: _____
(b) Organisational: _____
(c) Technical: _____
(d) Business: _____
(e) Political: _____
(f) Human factor: _____
(g) External: _____
(h) Other: _____

8. In view of the national context, please denote (with ***X***) the level of criticality to address each of the barriers enlisted above.

Type of barrier	Not critical	Irrelevant	Can benefit from some improvements	Necessary improvements should be made	Critical to address immediately
Legal					
Organizational					
Technical					
Business					
Political					
Human factor					
Other					

9. Please provide any further information, which in your opinion is important for our understanding of your country's context about the topics mentioned in this subchapter.

_____
_____
_____.

eIDAS v2: (European) Digital Identity Wallets

Enshrined in the Revised eIDAS Regulation is a recommendation for Member States to work towards the development of a Toolbox to support the implementation of the European Digital Identity framework. The scope of the toolbox should cover all aspects of the functionality of the European Digital Identity Wallets and of the qualified trust service for attestation of attributes as proposed by the Commission's proposal for a European Digital Identity framework. As the revised eIDAS is still not enacted, the aim of this section is to inspect the current state of the Member States in terms of existing Digital Identity Wallets solutions and readiness to act towards the implementation of the revised eIDAS Regulation.

1. Are there existing Digital Identity Wallets (DIWs) at this moment in your state, when eIDAS v2 has not been adopted yet?

- ○ Yes
- ○ No
- ○ No, but it is envisaged

Other: _____

If **Yes**, proceed with answering the next questions. Otherwise, move to the next section of the questionnaire.

Please name them and provide a reference accordingly:

	Name	Reference (Link, document, etc.)
DIW (1)		
DIW (2)		
DIW (3)		
DIW (4)		
DIW (5)		

2. Who is issuer of the DIWs in your country?

	Public entity	Private entity	Public-private partnership	Other
DIW (1)				
DIW (2)				
DIW (3)				
DIW (4)				
DIW (5)				

3. (Mark all that applies) The state provides validation mechanisms for the Digital Identity Wallets:

☐ To ensure its authenticity and validity can be verified
☐ To allow relying parties to verify that the attestation of attributes are valid
☐ To allow relying parties and qualified trust service providers to verify the authenticity and validity of attributed person identification data
☐ The State does not provide such mechanisms
☐ Other: _____

4. Are there means to ensure that the DIW is free of charge to natural persons?

○ Yes
○ No
○ Do not know

5. Please provide information on the following, if available:

- Number of citizens issued with DIWs: _____
- Number of businesses issued with DIWs: _____
- Number of citizens actively using DIWs: _____
- Number of businesses actively using DIWs: _____
- Number of issued identity credentials (attestations of attributes): _____
- Number of online service providers accepting DIWs and identity credentials (attestations of attributes): _____
- Number of online transactions by DIWs (total and cross-border):
  Total: _____ Cross-border: _____
- Share of online transactions requiring strong customer identification: _____
- % of individuals doing e-commerce (ratio of users of DIW doing e-commerce vs. total number of users of DIW x 100): _____
- % of individuals accessing online public services, if available (ratio of users accessing online public services vs. total number of users of DIW x 100): _____

6. Are there accredited bodies that certify the conformance of the DIWs with the requirements laid down in the relevant paragraphs of article 6a) from the eIDAS v2?

○ Yes
○ No
○ Do not know

If **Yes**, please state how many of them are private, and how many are public:

Private: _____
Public: _____

7. Indicate the types of drivers that you see important for the implementation of the DIWs in your country:

(a) Legal: _____
(b) Organisational: _____
(c) Technical: _____
(d) Business: _____
(e) Political: _____
(f) Human factor: _____
(g) External: _____
(h) Other: _____

8. In view of the national context, please denote (with *X*) the level of importance for each of the drivers listed above.

	FOR NATIONAL PURPOSES			**FOR CROSS-BORDER PURPOSES**		
Type of driver	***Desirable to exploit***	***Important to exploit***	***Critical to exploit***	***Desirable to exploit***	***Important to exploit***	***Critical to exploit***
Legal						
Organizational						
Technical						
Business						
Political						
Human factor						
Other						

9. Please provide any further information, which in your opinion is important for our understanding of your country's context about the topics mentioned in this subchapter.

_____
_____
_____.

1. Single Digital Gateway: Life Events

The Single Digital Gateway Regulation specifies a list of 21 procedures, covering the major life events of the EU citizens: Birth, Residence, Studying, Working, Moving, Retiring, Running a business. Please provide the current status of the digital presence and mobile availability of the 21 procedures in your country.

1. Please insert the required information on the mentioned procedures:

	Online authentication	Implementation of the OOP (data reuse)	Digitalised	Depends on procedure(s)[4]:
1.Requesting proof of registration of birth	Choose an item.	Choose an item.	Choose an item.	
2.Requesting proof of residence	Choose an item.	Choose an item.	Choose an item.	
3.Applying for a tertiary education study financing	Choose an item.	Choose an item.	Choose an item.	
4.Submitting an initial application for admission to public tertiary education institution	Choose an item.	Choose an item.	Choose an item.	
5.Requesting academic recognition of diplomas, certificates or other proof of studies or courses	Choose an item.	Choose an item.	Choose an item.	
6.Request for determination of applicable legislation in accordance with Title II of	Choose an item.	Choose an item.	Choose an item.	

[4] Denote by entering the number of the relevant procedures.

Regulation (EC) No 883/2004 (1)				
7.Notifying changes in the personal or professional circumstances of the person receiving social security benefits	Choose an item.	Choose an item.	Choose an item.	
8.Application for a European Health Insurance Card (EHIC)	Choose an item.	Choose an item.	Choose an item.	
9.Submitting an income tax declaration	Choose an item.	Choose an item.	Choose an item.	
10.Registering a change of address	Choose an item.	Choose an item.	Choose an item.	
11.Registering a motor vehicle originating from or already registered in a Member State	Choose an item.	Choose an item.	Choose an item.	
12.Obtaining stickers for the use of the national road infrastructure	Choose an item.	Choose an item.	Choose an item.	
13.Obtaining emission stickers issued by a public body or institution	Choose an item.	Choose an item.	Choose an item.	
14.Claiming pension and pre-retirement benefits from compulsory schemes	Choose an item.	Choose an item.	Choose an item.	
15.Requesting information on	Choose an item.	Choose an item.	Choose an item.	

the data related to pension from compulsory schemes				
16.Business activity: Notification, permission for exercising, changes and termination	Choose an item.	Choose an item.	Choose an item.	
17.Registration of an employer with compulsory pension and insurance schemes	Choose an item.	Choose an item.	Choose an item.	
18.Registration of employees with compulsory pension and insurance schemes	Choose an item.	Choose an item.	Choose an item.	
19.Submitting a corporate tax declaration	Choose an item.	Choose an item.	Choose an item.	
20.Notification to the social security schemes of the end of contract with an employee	Choose an item.	Choose an item.	Choose an item.	
21.Payment of social contributions for employees	Choose an item.	Choose an item.	Choose an item.	

2. Please insert the required information on the mentioned procedures:

	Mobile accessibility	**Online availability for cross border use**
Requesting proof of registration of birth	Choose an item.	Choose an item.

Requesting proof of residence	Choose an item.	Choose an item.
Applying for a tertiary education study financing	Choose an item.	Choose an item.
Submitting an initial application for admission to public tertiary education institution	Choose an item.	Choose an item.
Requesting academic recognition of diplomas, certificates or other proof of studies or courses	Choose an item.	Choose an item.
Request for determination of applicable legislation in accordance with Title II of Regulation (EC) No 883/2004 (1)	Choose an item.	Choose an item.
Notifying changes in the personal or professional circumstances of the person receiving social security benefits	Choose an item.	Choose an item.
Application for a European Health Insurance Card	Choose an item.	Choose an item.
Submitting an income tax declaration	Choose an item.	Choose an item.
Registering a change of address	Choose an item.	Choose an item.
Registering a motor vehicle originating from or already	Choose an item.	Choose an item.

registered in a Member State		
Obtaining stickers for the use of the national road infrastructure	Choose an item.	Choose an item.
Obtaining emission stickers issued by a public body or institution	Choose an item.	Choose an item.
Claiming pension and pre-retirement benefits from compulsory schemes	Choose an item.	Choose an item.
Requesting information on the data related to pension from compulsory schemes	Choose an item.	Choose an item.
Business activity: Notification, permission for exercising, changes and termination	Choose an item.	Choose an item.
Registration of an employer with compulsory pension and insurance schemes	Choose an item.	Choose an item.
Registration of employees with compulsory pension and insurance schemes	Choose an item.	Choose an item.
Submitting a corporate tax declaration	Choose an item.	Choose an item.
Notification to the social security schemes of the end of	Choose an item.	Choose an item.

contract with an employee		
Payment of social contributions for employees	Choose an item.	Choose an item.

3. What is the approximate percentage of procedures available digitally as compared to overall number of public, administrative services? (State N/A if not available)

at national level _____
at regional/local level _____
at cross-border level: _____

4. What is the approximate percentage of digital-only services (*services available exclusively online*)? (State N/A if not available)

at national level _____
at regional/local level _____
at cross-border level _____

5. Are there digital means of redress or appeal available in the event of disputes with competent authorities (as per Article 10(e) of Regulation (EU) 2018/1724)?

- ○ Yes
- ○ Yes, both at national and cross-border level
- ○ No
- ○ Do not know

If **Yes**, add a link or a reference to the service, if known: _____

6. What is the type and format of evidence to be submitted?

	Type	**Language**	**Format of the evidence**	**Origin of the evidence**
Requesting proof of registration of birth			Choose an item.	Choose an item.
Requesting proof of residence			Choose an item.	Choose an item.
Applying for a tertiary education study financing			Choose an item.	Choose an item.

Submitting an initial application for admission to public tertiary education institution			Choose an item.	Choose an item.
Requesting academic recognition of diplomas, certificates or other proof of studies or courses			Choose an item.	Choose an item.
Request for determination of applicable legislation in accordance with Title II of Regulation (EC) No 883/2004 (1)			Choose an item.	Choose an item.
Notifying changes in the personal or professional circumstances of the person receiving social security benefits			Choose an item.	Choose an item.
Application for a European Health Insurance Card			Choose an item.	Choose an item.
Submitting an income tax declaration			Choose an item.	Choose an item.
Registering a change of address			Choose an item.	Choose an item.
Registering a motor vehicle originating from or			Choose an item.	Choose an item.

already registered in a Member State				
Obtaining stickers for the use of the national road infrastructure			Choose an item.	Choose an item.
Obtaining emission stickers issued by a public body or institution			Choose an item.	Choose an item.
Claiming pension and pre-retirement benefits from compulsory schemes			Choose an item.	Choose an item.
Requesting information on the data related to pension from compulsory schemes			Choose an item.	Choose an item.
Business activity: Notification, permission for exercising, changes and termination			Choose an item.	Choose an item.
Registration of an employer with compulsory pension and insurance schemes			Choose an item.	Choose an item.
Registration of employees with compulsory pension and insurance schemes			Choose an item.	Choose an item.

Submitting a corporate tax declaration			Choose an item.	Choose an item.
Notification to the social security schemes of the end of contract with an employee			Choose an item.	Choose an item.
Payment of social contributions for employees			Choose an item.	Choose an item.

7. Can the procedures be carried out in other (than the MS national) language(s)?

○ Yes

○ No

○ Do not know

If Yes, please state in which language(s):

_____

_____

8. Are there applicable fees for carrying out any of the 21 procedures?

○ Yes (provide info): _____

○ No

○ Do not know

9. What online methods for national use canbe employed to pay the applicable fee?

☐ National banking solution
☐ Paypal
☐ Credit/debit card
☐ Do not know
☐ Other: _____

9. What online methods for cross-border use can be employed to pay the applicable fee?

☐ National banking solution
☐ Paypal

☐ Credit/debit card
☐ Do not know
☐ Other: _____

10. Does your MS make use of the Internal Market Information System (IMI), established by Regulation (EU) No 1024/2012? [for the purposes of notification and explanation of why physical presence might be required for the "fully-online" procedural steps (Article 6(4)) and for the Verification of evidence between Member States (Article 15)].

- ○ Yes, only for the purposes of notification and explanation of why physical presence might be required for the "fully-online" procedural steps
- ○ Yes, only for the Verification of evidence between Member States
- ○ Yes, for all relevant purposes
- ○ No
- ○ Do not know

Describe any specificities if IMI is being used: _____
_____
_____

11. Indicate the types of barriers that the implementation of the SDG procedures has encountered so far in your country and explain its implications:

(a) Legal: _____
(b) Organisational: _____
(c) Technical: _____
(d) Business: _____
(e) Political: _____
(f) Human factor: _____
(g) External: _____
(h) Other: _____

12. In view of the national context, please denote (with *X*) the level of criticality to address each of the barriers enlisted above.

Type of barrier	Not critical	Irrelevant	Can benefit from some improvements	Necessary improvements should be made	Critical to address immediately
Legal					
Organizational					
Technical					
Business					
Political					

Human factor					
Other					

13. Please provide any further information, which in your opinion is important for our understanding of your country's context concerning the topics mentioned in this subchapter.

_____
_____
_____.

Digital Service Infrastructures

The aim of this subchapter is to identify the advancement of Digital Service Infrastructures (DSIs). The DE4A project will be implemented in compliance with the existing DSIs, with the goal of delivering a network of public services available for citizens, businesses and public administrations.

1. Do you already have an eDelivery infrastructure set up in your MS?

- ○ Yes
- ○ No
- ◉ Do not know

Other: _____

3. How many eDelivery Gateways do you foresee to use for the SDG and Once-Only Technical System?

- ○ One
- ○ More
- ○ Do not know

Other: _____

4. Which type of gateway will you use for the SDG?

- ○ Domibus
- ○ Holodeck
- ○ Do not know
- ○ Not decided yet

Other: _____

5. Does your country participate in some of the European Blockchain Services Infrastructure (EBSI), H2020, CEF Digital or Recovery and Resilience Fund projects' use cases?

- ○ Yes
- ○ No
- ○ Do not know

Other: _____

If **Yes**, please indicate the name, status (planned, implemented, in production) and operational context (e.g. public procurement, internal financial audit etc.) of each of the use cases:

Name of use case	Status	Operational context

Other remarks: _____

6. Briefly explain the types of barriers that the implementation of the DSIs and the subservices have encountered in your country:

(a) Legal: _____
(b) Organisational: _____
(c) Technical: _____
(d) Business: _____
(e) Political: _____
(f) Human factor: _____
(g) External: _____
(h) Other: _____

7. In view of the national context, please denote (with *X*) the level of criticality to address each of the barriers enlisted above.

Type of barrier	Not critical	Irrelevant	Can benefit from some improvements	Necessary improvements should be made	Critical to address immediately
Legal					
Organizational					
Technical					
Business					
Political					
Human factor					
Other					

5. Please provide any further information, which in your opinion is important for our understanding of your country's context with regards to the topics mentioned in this subchapter.

_____
_____

Once-Only Principle and Data strategy

This part of the questionnaire inquires about the member states' implementation of the Once-Only Principle (OOP) and reuse of data principle. The OOP envisages reduction of administrative burdens for the EU citizens, businesses, institutions and public administrations by allowing them to provide a certain type of information once and implying the reuse of the collected data upon the consent of all parties.

1. Is there any national digital transformation strategy to push forth a set of strategic and tactical measures to support eGovernment development?

○ No

○ Do not know

○ Yes (please provide a link/reference to any relevant documentation):

_____

2. To what extent has your country adopted a national data strategy? Check all that apply.

☐ A strategy of reusing public sector data in the public sector
☐ A strategy for harmonization of data across selected registries
☐ A strategy for Open Data
☐ Implementation of Open Data by default
☐ One or more national catalogues of datasets to make data findable
☐ A national governance implementation supporting data access
☐ Other (please specify): _____

3. Which base registries implemented for national use can be accessed by private legal entities?

☐ Persons/citizens
☐ Vehicle
☐ Tax
☐ Businesses
☐ Addresses
☐ Building and housing
☐ Cadasters
☐ Geographical data
☐ Higher Education
☐ None
☐ Other (please specify) _____

4. What types of private companies can access base registries?

For personal data: _____
For non-personal data: _____

5. What are the access conditions?

_____

6. Please, indicate how the access to base registries is implemented. Check all that applies.

☐ Replication of registries to authorities that need access
☐ Data lookup supported by APIs
☐ Subscription of data for public services
☐ Access to base registries is subject to transactional fees
☐ Access to data services under authorization processes
☐ Other (please specify) _____

7. From the drop-down menu below, denote if there are any fees introduced for access to cross-border registries.

	Public organizations	**Private organizations**	**Citizens**
Fees for national transactions	Choose an item.	Choose an item.	Choose an item.
Fees for cross-border transactions	Choose an item.	Choose an item.	Choose an item.

Other (please specify) _____

8. What communication patterns are supported in the offering of public services in your country?

○ Synchronous (direct response to a request, typically within seconds)
○ Asynchronous (delayed response, hours or even days)
○ A mix of both
○ Do not know
Other: _____

9. Please check (with *X*) the types of personal information citizens can examine and verify the access to by public officials:

	Not implemented	Citizens can access their own data	Citizens can change (request a	Citizens can verify access to	Not applicable in my country	Do not know

			change of) their data	their data by others		
Personal file						
Tax declarations						
Medical file						
Cadasters (private property)						
Personal mandates						
None						

Other (please specify) _____

10. Mark (with *X*) the base registries for the relevant procedural requirements or preconditions for an exchange under the respective legislation:

	Persons/ Citizens	Vehicle	Tax	Businesses	Addresses	Building and housing	Cadasters	Geographical data	Higher Education	Other
No conditions[5]										
Prior request from the user										
Authorization must be written into the law										
Authorization must be obtained from an authority designated in the law										
Agreement between the sending and the receiving										

[5] Any party may receive and use our data as-is without restrictions or prior authentication (data is shared as open data)

administrations										
Obligation to use certain data formats										
Obligation for certain intermediary authorities to organise the exchanges										
Obligation to use certain security measures in relation to the data										
Limitations on the permitted use of the data										
Identity matching										
Record matching										

Other (please specify) _____

11. To what extent is OOP implemented in your country? Check all that applies.

- ○ Broadly at national level
- ○ In certain areas or organisations at national level
- ○ Broadly at regional level
- ○ In certain areas or organisations at national level
- ○ At all levels of power
- ○ Not implemented at all
- ○ Do not know

Other (please specify): _____

12. In what cross-border OOP initiatives is/has your country been involved? (E.g. TOOP, BRIS, SCOOP4C, ECRIS, CEF, SPOCS, ISA2, DE4A, etc.)

_____

_____

13. Do current national laws allow direct data exchange with a public administration from another Member State?

- ○ Yes
- ○ No
- ○ Do not know

If **Yes**, please provide answers to the following:

13a) Can this exchange happen directly based on the request from the foreign public administration without additional interaction with the user from the authority providing the evidence?

- ○ Yes
- ○ No
- ○ Do not know

13b) Is there a legal distinction between requests coming from public administrations in your own country as opposed to such from other countries?

- ○ Yes
- ○ No
- ○ Do not know

14. What other sources of OOP regulation exist in your country? Check all that apply.

☐ None
☐ Non-legislative measures (strategies, green / white papers, etc.)
☐ Written guidelines or recommendations
☐ OOP is an unwritten rule / practice
☐ Other (please specify): _____

15. How would you evaluate the general attitude and willingness in your country towards the following aspects of OOP?

	Public organizations	Private organizations	Citizens
Sharing data with public	Choose an item.	Choose an item.	Choose an item.

organizations within the country			
Sharing data with private organizations within the country	Choose an item.	Choose an item.	Choose an item.
Sharing data with other countries	Choose an item.	Choose an item.	Choose an item.
Sharing personal data with public organizations in the country	Choose an item.	Choose an item.	Choose an item.
Sharing personal data with private organizations in the country	Choose an item.	Choose an item.	Choose an item.
Sharing personal data with other countries	Choose an item.	Choose an item.	Choose an item.
Changing existing organizational processes, procedures and structures to enable OOP nationally	Choose an item.	Choose an item.	Choose an item.
Changing existing organizational processes, procedures and structures to enable cross-border OOP	Choose an item.	Choose an item.	Choose an item.
Changing existing technological solutions (information systems, architectures), etc. to enable	Choose an item.	Choose an item.	Choose an item.

OOP nationally			
Changing existing technological solutions (information systems, architectures), etc. to enable cross-border OOP	Choose an item.	Choose an item.	Choose an item.

16. How concerned are you with the effort and financial costs of adapting or implementing the following national parts of the OOP Technical System (mark the relevant choice with *X*):

	Not relevant	Very concerned	Somewhat concerned	Not concerned
eDelivery infrastructure				
Adaptation of procedures				
Adaptation of data sources				
Data service directory				
Semantic repository				
Evidence broker				
Auditing components				
Preview components				
Other:				

17. Please specify and assess the beneficial outcomes that have been observed so far for the national and the cross-border implementation of OOP.

	National implementation	Cross-border implementation
Increased efficiency	Choose an item.	Choose an item.
Administrative simplification	Choose an item.	Choose an item.
Automation of practices and processes	Choose an item.	Choose an item.
Time savings	Choose an item.	Choose an item.

Cost savings	Choose an item.	Choose an item.
Increased collaboration between agencies	Choose an item.	Choose an item.
Better governance	Choose an item.	Choose an item.
Avoidance of task duplication	Choose an item.	Choose an item.
Better data quality and reliability	Choose an item.	Choose an item.
Improved interoperability	Choose an item.	Choose an item.
Increased transparency and accountability	Choose an item.	Choose an item.
Fraud reduction	Choose an item.	Choose an item.
Increased digitalization and digitization	Choose an item.	Choose an item.

Other (please specify) _____

18. Indicate the types of barriers that the implementation of the OOP system and the data strategy have encountered in your country:

(a) Legal: _____
(b) Organisational: _____
(c) Technical: _____
(d) Business: _____
(e) Political: _____
(f) Human factor: _____
(g) External: _____
(h) Other: _____

19. In view of the national context, please denote (with *X*) the level of criticality to address each of the barriers enlisted above.

Type of barrier	Not critical	Irrelevant	Can benefit from some improvements	Necessary improvements should be made	Critical to address immediately
Legal					

Organizational					
Technical					
Business					
Political					
Human factor					
Other					

20. Please provide any further information which, in your opinion, is important for our understanding of your country's context with regards to the topics mentioned in this subchapter.

_____
_____.

Contact information

Please provide contact details of people (name, email and/or phone number) who we could contact in case we would need some additional clarification or for the purpose of a personal interview:

_____
_____.