D1.7 Legal, technical, cultural and managerial risks and barriers

Document Identification			
Status	Final	**Due Date**	31/07/2020
Version	1.1	**Submission Date**	16/04/2021

Related WP	WP2, WP3, WP4, WP5 & WP6	**Document Reference**	D1.7
Related Deliverable(s)	D1.1, D1.2, D1.3, D1.4, D1.5, D1.6, D1.8 & D2.3	**Dissemination Level (*)**	PU
Lead Participant	DIGST	**Lead Author**	Lasse Kramp (DIGST)
Contributors	Lasse Kramp (DIGST); Sven Rostgaard Rasmussen (DIGST); Momme Nommensen (DIGST)	**Reviewers**	Arvid Welin (SU) Dan Crisfalusi (CIO); Fraga Tariuc (CIO)

Keywords :
Risks and barriers on cross-border digital European services, EIF interoperability framework, Once Only, eGovernment,

Document Information

List of Contributors	
Name	Partner
Alberto Crespo	ATOS
Alenka Žužek Nemec	SI-MPA
Ana Rosa Guzman Carbonell	MPTFP-SGAD
Arvid Welin	SU
Carl-Markus Pisswanger	BRZ
Dan Crisfalusi	CIO
Eddy Corthouts	BOSA
Ekaterina Fedko	BOSA
Frank Leyman	BOSA
Gérard Soisson	CTIE
Gertjan Bouwers	MinBZK
Hans Ekstål	BVE
Hans Graux	time.lex
Ivar Vennekens	RVO
Jose Antonio Eusamio Mazagatos	MPTFP-SGAD
Lasse Kramp	DIGST
Laura de Zulueta	MPTFP-SGAD
Malin Norlander	BVE
Marc Bruyland	BOSA
Matthias Lichtenthaler	BRZ
Momme Nommensen	DIGST
Sofia Paredes	AMA
Sven Rostgaard Rasmussen	DIGST

Document History			
Version	Date	Change editors	Changes
0.2	24/06/2020	Momme Nommensen (DIGST)	Table of contents
0.5	14/08/2020	Sven Rasmussen (DIGST)	Version submitted for internal review
0.6	24/08/2020	Momme Nommensen (DIGST)	Revision of chapters 1-3
0.7	26/08/2020	Sven Rasmussen (DIGST)	revised chapters 4
0.7.1	26/08/2020	Lasse Kramp (DIGST)	Revised executive summary and chapters 5-6
0.8	27/08/2020	Momme Nommensen (DIGST)	Editorial changes
0.9	27/08/2020	Lasse Kramp (DIGST)	Version submitted for quality control
0.9.1	28/08/2020	Lasse Kramp (DIGST)	Editorial changes and revised executive summary

Document History			
1.0	31/08/2020	Julia Wells (Atos)	Final version for submission
1.1	06/04/2021	Atos	Update following on first interim review recommendations. Clarification that WP1 deliverables are designed to be stand-alone, which causes some repetition between deliverables

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Sven Rostgaard Rasmussen, Lasse Kramp (DIGST)	28/08/2020
Quality manager	Julia Wells (ATOS)	28/08/2020 and 06/04/2021
Project Coordinator	Ana Piñuela Marcos (ATOS)	31/08/2020 and 15/04/2021

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
CIO	Chief Information Officer
DC	Data Consumer
DESI	Digital Economy and Society Index
DP	Data Provider
DSI	Digital Service Infrastructure
Dx.y	Deliverable number y, belonging to WP number x
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
LOST	Legal, Organisational, Semantic and Technical interoperability
Lx	Legal risk or barrier number x
MS	Member State
OOP	Once Only Principle
OOTS	Once-Only Technical System
Ox	Organisational risk or barrier number x
PID	Personal identifier
ROI	Return of investment
SDG	Single Digital Gateway
SDGR	Single Digital Gateway Regulation
SEMPER	Secure Electronic Marketplace for Europe
Sx	Semantic risk or barrier number x
TOOP	The Once Only Project
Tx	Technical risk or barrier number x
WP	Work Package

Executive Summary

The project Digital Europe for All (DE4A) was launched in January 2020 as a result of collaboration of 27 organizations from 11 countries of the European Union. The project is funded by the EU Horizon 2020 research and innovation Framework Programme and is aimed to create an inclusive digital Environment in Europe ensuring the Single Digital Market rights of citizens and businesses by building on secure, privacy-preserving and trustworthy realisation of fundamental once-only, relevant-only and digital by default principles. The DE4A large-scale pilot reinforces the connectivity of national digital endeavours and, building upon the existing infrastructure, it attempts to contribute to an overarching eGovernment network for Europe supporting parallel efforts from the EC and the Member States to realise the Once-Only Principle Technical System in compliance with Single Digital Gateway and aligned with EU eGovernment Action Plan 2016-2020, Tallinn Declaration and EIF Implementation Strategy.

"D1.7 Legal, technical, cultural and managerial risks and barriers" is one of the formal outputs of WP1 "Inventory of current eGovernment landscape" for the DE4A project. This workpackage which aims to take stock of the existing situation of the deployment of cross-border integrated Digital European Public Services in the Member States participating in DE4A, has produced four deliverables in the first period:

- D1.1 Member state eGoverment Baseline (June 2020)
- D1.3 Member State Once Only and data strategy Baseline (June 2020)
- D1.5 Baseline EU Building Blocks supporting Once Only and standard data sharing patterns (June 2020)
- D1.7 Legal, technical, cultural and managerial barriers (August 2020)

All four documents are conceived as stand-alone documents. This facilitates reading the document of interest but leads to some level of repetition between documents, in particular regarding the sections on theoretical background and methodology.

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. 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.

In order to ensure a broad spectrum of risks and barriers are identified and properly understood, the study draws upon three different kinds of sources: A survey among the Chief Information Officers of the EU and EFTA Member States, a literature review of European projects, and focus group interviews with a dozen experts from 10 different countries.

By applying the framework of the LOST interoperability layers from the EIF conceptual model for integrated services, the report identifies and describes 38 risks and barriers across the four layers of interoperability. For each risk and barrier, drivers and enablers that may potentially mitigate the risk or overcome the barrier are presented.

The report finds that when evaluating the probability and consequence of each risk and barrier, 32 of the 38 risks and barriers are critical to address in order to be able to successfully move forward with the implementation of cross-border integrated digital public services. Furthermore, the study shows that most risks and barriers are widespread among the EU and EFTA Member States.

The study also identifies critical risks and barriers at all levels of interoperability such as lack of legal basis for exchanging data and secure user identity management; organisational barriers on sharing of data and integrated public service governance; semantic barriers in terms of missing harmonisation of criteria, evidences, and identity/user-rights management; technical barriers on integration with

sectoral and national systems and governance of distributed systems. According to the study, organisational risks and barriers are the most prevalent issue and each risk or barrier often has implications on other layers, or conversely may have solutions coming from the other layers, adding further complexity.

On that basis, the report discusses how the development and implementation of cross-border digital public services may best be supported and suggests an increased focus on organisational barriers, including supporting national digitisation efforts with high return on investment.

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 to provide a meaningful and valuable purpose. Especially in a context of political prioritisation 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 said 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 digitalisation in Europe. Hence, this study is a complementary extension of the previous deliverables within the same work package consisting of:

- D1.1 Member State eGovernment Baseline (June 2020), which elaborates on the current advancement of the existing eGovernment landscape
- D1.3 Member State Once Only and data strategy baseline (June 2020), which elaborates on the current advancement of data strategy and Once Only implementation
- D1.5 EU Baseline Building Block Catalogue (June 2020), which identifies main existing building blocks from EU programmes and projects that can enable Once Only implementation and relevant standard data sharing

Complementary, the four reports of the work package deliver a comprehensive, multifaceted view on the existing infrastructures, practices, expected benefits and barriers on cross-border digitalisation 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 digitisation efforts on national and European scales. They are designed as stand-alone documents, and so necessarily contain some repetition regarding background and methodology.

Each of the studies will be updated during the course of the project.

1.2 Structure of the document

This document is divided into 6 main sections:

- Chapter 1 (Introduction) gives introductory context and theoretical background to the matter of the deliverable;
- Chapter 2 (Methodology) elaborates on the utilised methodology and limitations;
- Chapter 3 (Survey) presents the results of the DE4A survey;
- Chapter 4 (Risks and barriers) describes the identified risks and barriers;
- Chapter 5 (Discussion) discusses the found results in an aggregated format;
- Chapter 6 (Conclusions) provides concluding remarks on the research.

The document additionally includes the following annexes:

- Annex I. Calculation Methodology
- Annex II. Digital Europe for All (DE4A) survey

1.3 Background

Rapid development of information and communication technologies has given a significant impetus to the transformation of public administration and set eGovernment on the political agenda of the European Union (EU) and European Free Trade Association (EFTA).

Formulation of the first large scale eGovernment Action Plan 2011-2015 articulated the necessity for political mobilisation of digital transformation and became one of the milestones towards the establishment of a collaborative network of the EU Member States (MS) in the area of government digitalisation [1]. The termination of the Action Plan coincided with the adoption of the Digital Single Market Strategy, which put forward the necessity to establish seamless functioning of public administration in a cross-border perspective, easing access to public services for citizens and businesses. The new eGovernment Action Plan 2016-2020, building upon the previous achievements in cross-border environment, underpins user-centricity as one of its main objectives and sets the strategic direction for the current digital initiatives in Europe [2]. The Tallinn Declaration on eGovernment from 2017 complements the undertaken strategy and elaborates on the principles of digital transformation of public administration [3]. Reinforcing the reduction of administrative burden on citizens and businesses, the adopted strategies and declarations establish the Once Only Principle (OOP) as one of the central elements for development of the Digital Single Market.

As different studies on eGovernment suggest, there is an uneven level of eGovernment advancement across the EU MS. Despite the availability of the common regulatory framework and the launch of large-scale cross-border projects, reports on eGovernment Benchmark demonstrates some countries having a higher adoption rate of eID adoption and availability of public services in a cross-border perspective [4]. The Digital Economy and Society Index similarly depicts unequal coverage of internet connectivity and availability of public digital services across Europe [5]. These differences are essential for comprehension of the current European eGovernment landscape.

In light of the goal of creating a single digital space of Europe, the project DE4A aims to create an inclusive digital environment for the EU citizens and businesses. Supporting the EU Public Administration in addressing the existing challenges to the implementation of the digital cross-border initiatives, the DE4A contributes to the realisation of the aforementioned Tallinn Declaration and EU eGovernment Action Plan 2016-2020 as well as the Single Digital Gateway Regulation (SDGR) [6] and European Interoperability Framework (EIF) Implementation Strategy [7]. As articulated in the project proposal, the goal of the DE4A is to:

"reinforce trust in public institutions and to unleash multiple measurable positive impacts in terms of efficiency gains and reduction of current administrative burden and costs, rooted on a Toolkit for extended semantic interoperability and on secure, privacy-preserving and trustworthy realization of fundamental Once-Only, relevant-only and digital by default principles, through state-of-the-art, usable and high-quality fully online procedures accessible through the Single Digital Gateway (SDG)".

2 Methodology

2.1 Approach

As stated in the introduction, the purpose of this report is to identify risks and barriers on the implementation of cross-border integrated digital European Services. Without specification of the timeframe, area or depth of such implementation, the ambition may be understood as a continuous development of the scope of the SDGR, in terms of broadening the number of areas as well as a deepening the services within each area.

Where the SDGR employs a user-centric focus to ease cross-border users' access to public services, a development of 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 organisational 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 different variations of the identified risks and barriers.

Despite the abovementioned limitations on the direct applicability of all the risks and barriers to every scenario, for the purpose of operationalisation, the services included in SDGR 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.

Risks and barriers often influence several aspects at the same time, often in a chicken-and-egg manner, making it difficult to differentiate clearly between cause and effect. Furthermore, aspects of legal, technical, cultural and managerial issues often interplay in complex relationships.

In order to be able to apply conceptual accuracy to the understanding and consequent identification and description of the risks and barriers on the deployment of integrated services, the EIF conceptual model for integrated public services is applied as a framework for categorisation. The model consists of legal, organisational, semantic and technical interoperability layers.

As the four aspects in focus of this study only partially correspond to the four layers of the EIF-model, the aspects were converted as follows: "Legal" and "technical" were converted directly to their respective counterparts, "cultural" and "managerial" are treated as "organisational" issues, and finally a "semantic" interoperability layer is added to the analysis. The EIF model is often abbreviated as the LOST-model and described in further detail in section 2.4.

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 have been applied:

- A **risk** is understood as something that may happen and which has an adverse effect on the desired outcome if it were to happen.
- A **barrier** is understood as something, which by its current presence or lack thereof has an adverse effect on the desired outcome.
- A **driver** is understood as an incentive to make something happen. A driver may have a positive effect on the desired outcome, or conversely counter a negative effect. In principle, a driver may also have a negative effect on the desired outcome. Drivers may be generic, like political or societal changes, or specific, like increased costs of supporting manual processes for cross-border services.

- An **enabler** is understood as 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.

2.2 Scope

In the context of the purpose of this report as described in chapter 1.1 and the other studies in the series, the present study focuses on the legal, technical, cultural and managerial risks and barriers on the implementation of cross-border integrated digital public services.

However relevant for determining the volume, timeframe and content of the cross-border services to be implemented, negotiations leading up to agreements on e.g. new regulation, strategies or initiatives are beyond the scope of this study.

Furthermore, although some issues are also complemented with views on the private sector, the identification of risks and barriers focuses primarily on issues relevant for the public sector.

The geographical scope of the study covers the EU and EFTA MS.

2.3 Data collection

As risks and barriers may play out very differently in different national contexts and as such may be difficult to get a clear picture of, a multi-disciplinary approach to gathering data has been taken in order to ensure that the conclusions are based on solid empirical grounds. As such, three types of sources have been used:

- **A survey** was conducted among the chief information officers (CIO) of all the EU and EFTA countries to identify the issues faced by those responsible for MS' strategy and implementation. The survey data is described in its own right in chapter 3, and findings from the survey in terms of specific risks and barriers are carried into chapter 4, where they are described in further detail.
  For the survey, the data collection was carried out by means of a joint survey questionnaire (see Annex II.) for deliverables D.1.1, D1.3, and D1.7 (present study), and was sent to 31 state representatives. It targeted the current eGovernment advancement of European states and consisted of four major subjects: Electronic Identification and Trust Services, Single Digital Gateway, Digital Service Infrastructure, and Once Only Principle and Data Strategy. Of these, the present study investigates the questions related to the perceived benefits of and barriers on implementation of the Once Only Principle and Data Strategy. The online survey was disseminated among CIOs of the EU MS and EFTA countries and the data was collected between 1 and 24 April 2020. The respondents were requested to self-evaluate the performance of their countries with respect to the indicated topics. Acknowledging the challenge of gathering multifaceted information on eGovernment performance aggregated at the national level, where exact data was not available, respondents were suggested to provide their personal estimates. Furthermore, 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. Responses were received from 24 countries, corresponding to 77.5% of EU and EFTA countries: Austria, Belgium, Bulgaria, Croatia, Denmark, Finland, Germany, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland. The response rate for the countries participating in the pilot projects reached 100%, offering a solid ground for informed development of the pilots announced under the DE4A.

Driven by the goal of the DE4A, the survey questions were based on the outlined scope of the project. They were subsequently adjusted based on the availability of the relevant recent information on the subject in other reports and studies, such as eGovernment Benchmark reports [4], the Digital Economy and Society Index [5] and NIFO factsheets [13].
The data was cleansed and checked against the respondents' comments for the purpose of making possible adjustments prior to the analysis to ensure consistent quality of data. If needed, direct communication was undertaken to clarify the position of a respondent on a specific question.
As the total number of respondents is below 30, each answer influences the overall results. In order not to introduce additional risks of bias in the reporting, the answers given are reported directly in either absolute numeric values or percentages. Please see the exhaustive list of the calculations per graph in Annex I. Calculation Methodology.

- The second source of data is a **literature review** of large-scale European projects to ensure that existing knowledge is used. The Once Only Project (TOOP) [14] and Secure Electronic Marketplace for Europe (SEMPER) [15] hold valuable knowledge about different aspects of developing and implementing cross-border services. Finally, DE4A is used as a source of barriers, because it is a large-scale project aimed at implementation in real-life production settings across several countries. As such, the insights, the project offers, are derived from various perspectives. On one side generic legal white papers and on the other side actual problems stemming from real circumstances in the different piloting countries.
  Findings from the review are reported as an integral part of the descriptions of risks and barriers in chapter 4.
- Finally, as a third source of data, two **interviews were conducted with a focus group of experts** from the countries involved in DE4A WP1, in order to complement and validate early findings. The purpose of the group interviews was to cater for expert opinions as well as to include contributions related to challenges identified in the MS. The two interviews were held as 2-hour videoconferences with a week apart in July 2020.
  Prior to the first session, participants received an initial draft list of barriers on cross-border service implementation. The list was compiled on the basis of expressed considerations of DE4A participants to the draft SDGR architecture blueprint. On that basis, barriers and enablers of integrated public cross-border services were discussed during the meeting. As the interviews where held within a limited timeframe, the process has included incorporation of some additional written contributions from participating experts. The contributions are reported as an integral part of the descriptions of risks and barriers in chapter 4. Further, the experts were consulted with the charts based on the data from the DE4A survey presented in chapter 3. Their input and comments have been incorporated in the respective sections.

2.4 EIF Conceptual Model for integrated public services

The EU's internal market guarantees the free movement of goods, capital, services and people. People are free to work and relocate and businesses are free to trade and operate in all EU MS. In doing so, they inevitably have to interact electronically with several MS' public administrations. However, the modernisation of those administrations implies a risk of creating isolated digital environments and consequently electronic barriers. For this reason, efforts to digitise the public sector should be well coordinated to avoid digital fragmentation of services and data.

In what follows, the present report will consider the EIF Conceptual Model for integrated public services as a framework for compiling an inventory of contemporary legal, technical, cultural and managerial risks and barriers. In doing so, the reader will gain a more comprehensive understanding of the interoperability elements that help identify the barriers for the deployment of cross-border integrated Digital European Public Services.

EIF [12] gives specific guidance on how to set up interoperable digital public services. Its current version provides 47 concrete interoperability recommendations, with a strong focus on openness and information management, data portability, interoperability governance, and integrated service delivery. Hence, EIF offers public administrations advice on how to improve governance of their interoperability activities, establish cross-organisational relationships, streamline processes supporting end-to-end digital services, and ensure that neither existing nor new legislation compromise interoperability efforts. This is the result of taking into account new EU policies, such as the revised Directive on the reuse of Public Sector Information [8], the INSPIRE Directive [9], and the eIDAS Regulation [10] as well as newer EU initiatives, such as the European Cloud Initiative [11], the EU eGovernment Action Plan 2016-2020, and the Single Digital Gateway.

EIF is meant to be a generic framework that lays out the basic conditions for achieving interoperability, acting as the common denominator for relevant initiatives. In doing so, it provides a layered interoperability model, which organises different interoperability aspects to be addressed when designing public services. The model should be considered applicable to all digital public services and is considered an integral element of the interoperability-by-design paradigm. The paradigm is depicted in Figure 1 below and consists of three main elements:

- Interoperability Governance as a background layer;
- Integrated Public Service Governance as a cross-cutting component;
- and four layers of interoperability.

Figure 1 EIF interoperability model

Figure source: New European Interoperability Framework [12]

Interoperability governance is the key to a holistic approach and refers to the ability to decide on interoperability frameworks, institutional arrangements, organisational structures, roles and responsibilities, policies, agreements and other aspects of ensuring and monitoring interoperability. An example hereof, is the aforementioned INSPIRE Directive.

Integrated Public Service Governance ensures interoperability and coordination over time when operating and delivering integrated public services by putting in place the necessary governance structure. When multiple stakeholders are involved, there is a need for coordination and governance by the authorities with a mandate for planning, implementing and operating European public services. Finally, the model outlines **four layers** of legal, organisational, semantic and technical interoperability, that allow a more detailed analysis of specific barriers. As such, the present study will consider the four layers as a framework, when compiling the inventory of existing interoperability barriers. Often abbreviated as the LOST-model, the four layers are summarised with recommendations in Table 1 below.

Table 1 Four layers of interoperability

Layer	Description and recommendations
Legal	Public administrations contributing to the provision of a European public service work within their own national legal framework. Legal interoperability is about ensuring that organisations operating under different legal frameworks, policies and strategies are able to work together. This might require that legislation does not block the establishment of European public services within and between MS and that there are clear agreements about how to deal with differences in legislation across-borders, including the option of putting in place new legislation.
	Recommendations: • Ensure that legislation is screened by means of "interoperability checks", to identify any barriers to interoperability. When drafting legislation to establish a European public service, seek to make it consistent with relevant legislation, perform a "digital check" and consider data protection requirements.
Organisational	Organisational interoperability refers to the way in which public administrations align their business processes, responsibilities and expectations to achieve commonly agreed and mutually beneficial goals. In practice, organisational interoperability means documenting and integrating or aligning business processes and relevant information exchanged. Organisational interoperability also aims to meet the requirements of the user community by making services available, easily identifiable, accessible and user-centered.
	Recommendations: • Document your business processes using commonly accepted modelling techniques and agree on how these processes should be aligned to deliver a European public service. • Clarify and formalise your organisational relationships for establishing and operating European public services.
Semantic	Semantic interoperability ensures that the precise format and meaning of exchanged data and information is preserved and understood throughout exchanges between parties, in other words 'what is sent is what is understood'.
	Recommendations: • Perceive data and information as a public asset that should be appropriately generated, collected, managed, shared, protected and preserved. • Put in place an information management strategy at the highest possible level to avoid fragmentation and duplication. Management of metadata, master data and reference data should be prioritised. • Support the establishment of sector-specific and cross-sectoral communities that aim to create open information specifications and encourage relevant communities to share their results on national and European platforms.
Technical	Technical interoperability covers the applications and infrastructures linking systems and services. Aspects of technical interoperability include interface specifications, interconnection services, data integration services, data presentation and exchange, and secure communication protocols. A major obstacle to interoperability arises from legacy systems. Historically, applications and information systems in public administrations were developed in a bottom-up fashion, trying to solve domain-specific and local problems. This resulted in fragmented information and communications technology islands, which are difficult to interoperate.
	Recommendations: • Use open specifications, where available, to ensure technical interoperability when establishing European public services.

Table source: New European Interoperability Framework [12]

2.5 Methodological limitations of the study

Any type of data collection carries its own advantages and limitations. As a consequence, several different types of sources have been specifically chosen and explored to counter each other's shortcomings, in order to provide a solid empirical ground for the identification of risks and barriers. Nonetheless, the methodological limitations of each are still relevant to bear in mind, individually and collectively.

Regarding the survey, this method of collecting data, based on self-reporting, carries risks of bias, as respondents may over-report positive behaviour or conversely under-report negative behaviour to gloss over the country's actual status. This risk of bias was mitigated by not asking for the official position of the state combined with assuring no individual answers would be published, hereby relieving any perceived pressure to perform. As the number of e.g. "Do not know"-replies vary greatly, ranging up to 71% of the replies given to a certain question, the approach appears to have been successful.

Furthermore, as respondents were suggested to provide personal estimates where exact data was not available, replies may inadvertently be incorrect. However, the risk of such errors substantially altering overall replies is considered small, as the chosen respondents are experienced, high-ranking officials of the executive digitalisation authorities that may be considered generally knowledgeable about the subjects. Furthermore, the high response rate provides a substantial counterweight to such errors, if their allocation across questions and respondents may be presumed equally distributed.

Nonetheless, the aforementioned inherent risks of bias and erroneous replies, cannot be removed completely, and any conclusions based on the findings of the study should take into account the likelihood and implications of those risks.

Regarding the possibility of extrapolating results, despite the survey achieved a 77.5% response rate of the total population of countries, the study cannot be assumed to be exhaustive for the entire population of countries within the geographical scope. However, although the data does not provide sufficient methodological grounds for extrapolating the results to the entire population of EU and EFTA countries, no easily identifiable common denominator of the abstaining countries was found, giving no reason to believe that responses from these countries would be significantly different in general from the ones received.

Finally, the data from the survey does not provide grounds to infer hard conclusions about neither rationale behind the status nor time horizon for future development. As such, adoption and implementation levels may rise significantly over the next few years or be at a complete stand still.

Regarding the literature review, the primary defect is that it may be difficult to get a complete picture of risks and barriers on each of the projects merely by their official documentation. As with any kind of written material, some things are left out or documented in a skewed manner. Reasons for this may be simply that they have been forgotten at the time of writing, that they are thought to be of minor importance, because they may not have been the focus of the documentation, that the actual circumstances of the matter are too complex to communicate in an understandable way or in some cases that they are glanced over. Hence, without actually taking part in the processes, there is no way of knowing to which degree the documentation reflects the actual risks and barriers on a project or if other barriers could have been of relevance.

In addition to this, the reader must often interpret the documentation, which of course carries with it the risk of misinterpretation. When used as a single source of documentation, there is no way for a reader to clarify possible misunderstandings or dive deeper into specific issues of interest. Instead it must be taken at face value. However, the abovementioned risks have been mitigated to some extent by validating the findings with expert interviews, especially because some of the experts have in depth knowledge of the projects.

Regarding the expert contributions, both of the interviews were conducted within a rather limited timeframe. This meant that the focus group did not have the opportunity to take into account the actual progress of the report or comment barriers that were identified after the interviews had taken place. As such, the report lacks a final validation by the experts of the final version of the report.

Furthermore, conducting the interviews as focus group sessions has the advantage that it sparks discussions, and allows different people to complement each other. However, it does also have the disadvantage that some views or aspects may not be properly covered, as some may not feel quite comfortable discussing specific matters in a group. As the experts are all experienced in their field, all knew each other from the DE4A project, and the subject is not considered especially sensitive in general, this risk of someone holding their tongue is not considered to have played any substantial role in the interviews.

3 Survey

This chapter addresses different insights relevant for legal, technical, cultural and managerial risks and barriers derived from the DE4A survey[1]. As mentioned in chapter 2.3, the sections are based on data from the survey distributed to the CIOs of the EU and EFTA countries. The response rate was 77.5%, granting the study a solid basis for reporting on the actual status of the domains in focus.

The first two sections of this chapter render the findings from the project deliverables D1.1 *Member State eGovernment baseline* and D1.3 *Member State and Once Only and data strategy baseline*. Please see the respective reports for additional information, in depth descriptions and graphs on the subjects described in these sections. The latter sections are based on previously uncovered data from the same survey.

3.1 eGovernment baseline (barriers derived from D1.1)

The eID schemes – one of the cornerstones of the cross-border functioning of eGovernment systems – have been unequally implemented across the EU. The research suggests that only one third of the eID schemes have been (pre-)notified under the eIDAS regulation, whilst over 90 percent of the responding countries confirmed availability of a national eID scheme. The national eIDAS-Nodes similarly demonstrate asymmetric readiness for cross-border use, being more advanced in terms of accepting foreign eID-schemes for national use rather than supporting national eIDs abroad. Contrary to this, the implementation of trust services has demonstrated a rather homogenous spread across the participating countries.

The Digital Service Infrastructures (DSI) envisaged in the Connecting Europe Facility, have likewise showed different scale of implementation of both domain-specific and domain-independent building blocks. Whilst some DSIs have been widely set on technical implementation in the EU, 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 SDGR have similarly exposed significant differences in term of possibility for eID-authentication, mobile accessibility, applicability of the OOP and availability for cross-border use. Whilst showing generally high availability of the services for use with mobile devices, only approximately half of the services were accessible with the eID and enabled for cross-border use.

Providing the respondents with a possibility to leave context-relevant remarks for comprehension of eGovernment strategy, the study discovered dependency 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 early stage of regulatory development of some states. The study also notes different level of involvement of the private sector, detecting its interconnectedness with the eGovernment advancement.

3.2 Once Only and data strategy baseline (barriers derived from D1.3)

In regard to data strategy and generic access to base registries, the study shows that 50 percent of the responding countries report not having in place a strategy for reusing public sector data. Furthermore, only few of the base registries are generally accessible by private entities.

[1] See Annex II. Digital Europe for All (DE4A) survey

The study also shows that transaction fees are implemented in as much as nearly 60 percent of the countries for private entities. Although the equivalent numbers for public entities are somewhat lower, transactional fees are prevalent and as such, the report concludes, likely to have an adverse effect on the flow of data and hence the realisation of user benefits of the SDG.

Whilst the study reports a positive picture on citizens' access to their own data, the ability for citizens to gain insight into civil servants' access to their data is shown to be rare. Current levels of the implementation levels of the OOP are shown to be rather low in light of the time horizon for implementing the SDG. The deficiency was identified on regional as well as national levels, and despite implementation levels of the procedures related to the 21 life events of the SDG were slightly better, the overall picture remains one of low adoption and implementation. As differences in countries' administrative procedures and in the data required for those procedures may reasonably be assumed to add complexity, consequences of that deficiency may be expected to be even more prominent in a cross-border setting.

The study concludes that the status on data harmonisation, free and effective access to data, implementation of the OOP in national and cross-border services and the availability of those services for cross-border use, show severe shortcomings and must be improved drastically within the next three years for the SDG to be implemented as envisaged. As such, any initiative that utilises or depends on cross-border OOP should take into account that implementation of the OOP should not be taken for granted.

3.3 Benefits of implementing Once Only

The implementation of the OOP is expected to yield beneficial outcomes for the end user, whilst at the same time affect digital public services. Further, the beneficial outcomes will increasingly affect the European public administrations. Figure 2 below 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.

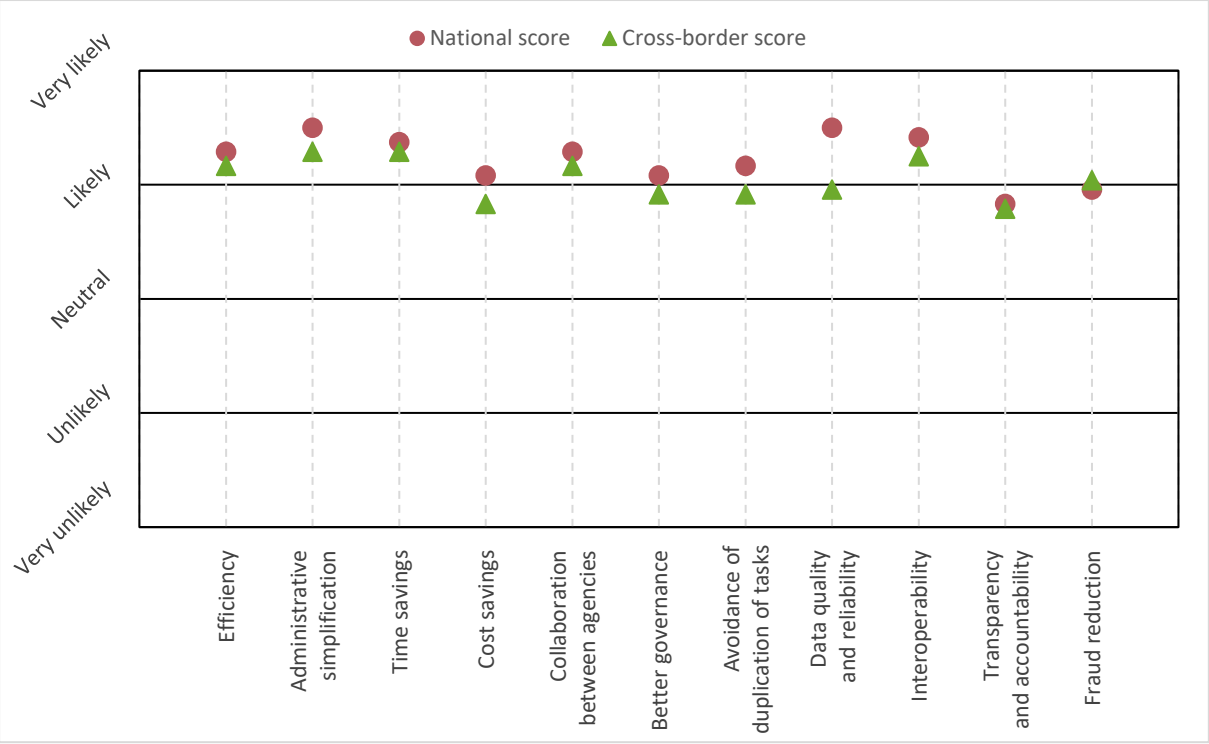

Figure 2 Average expected benefits of OOP implementation

In most cases, the responding countries expect the beneficial outcomes to be more likely on a national level compared to cross-border likeliness. Albeit, with the exception of data quality and reliability, the differences in likelihood are generally small.

Another interesting factor is fraud reduction. Examined closely, it can be observed that the responding countries actually expect benefits to be more likely in a cross-border context, than in a national context. It is worth noting, however, that the cross-border score is relatively equal to the other cross-border scores, whereas the national score is somewhat lower than the other national scores. As such, the reason behind the close scores is likely connected to nationals efforts to reduce fraud.

Since there are on average only marginal differences between the likeliness of expected benefits on a national and cross-border level, it is necessary to display the data in more detail. Figure 3 below shows the respondents' view on the beneficial outcomes of national and cross-border implementation of OOP in absolute numbers. For each of the types of outcomes, the views on benefits of national implementation are depicted in the upper bars, followed by views on benefits of cross-border implementation in the patterned bars below. The chart underlines that the overall picture shows a very high expectancy of perceived benefits of OOP in a national and a cross-border context. As such, half or more of the respondents regard all of the types of outcomes to be likely or very likely. Some of the types even reach the 75 percent likelihood.

However, the chart also shows that a rather large portion of the respondents, up to 40%, have a neutral perception of expected benefits.

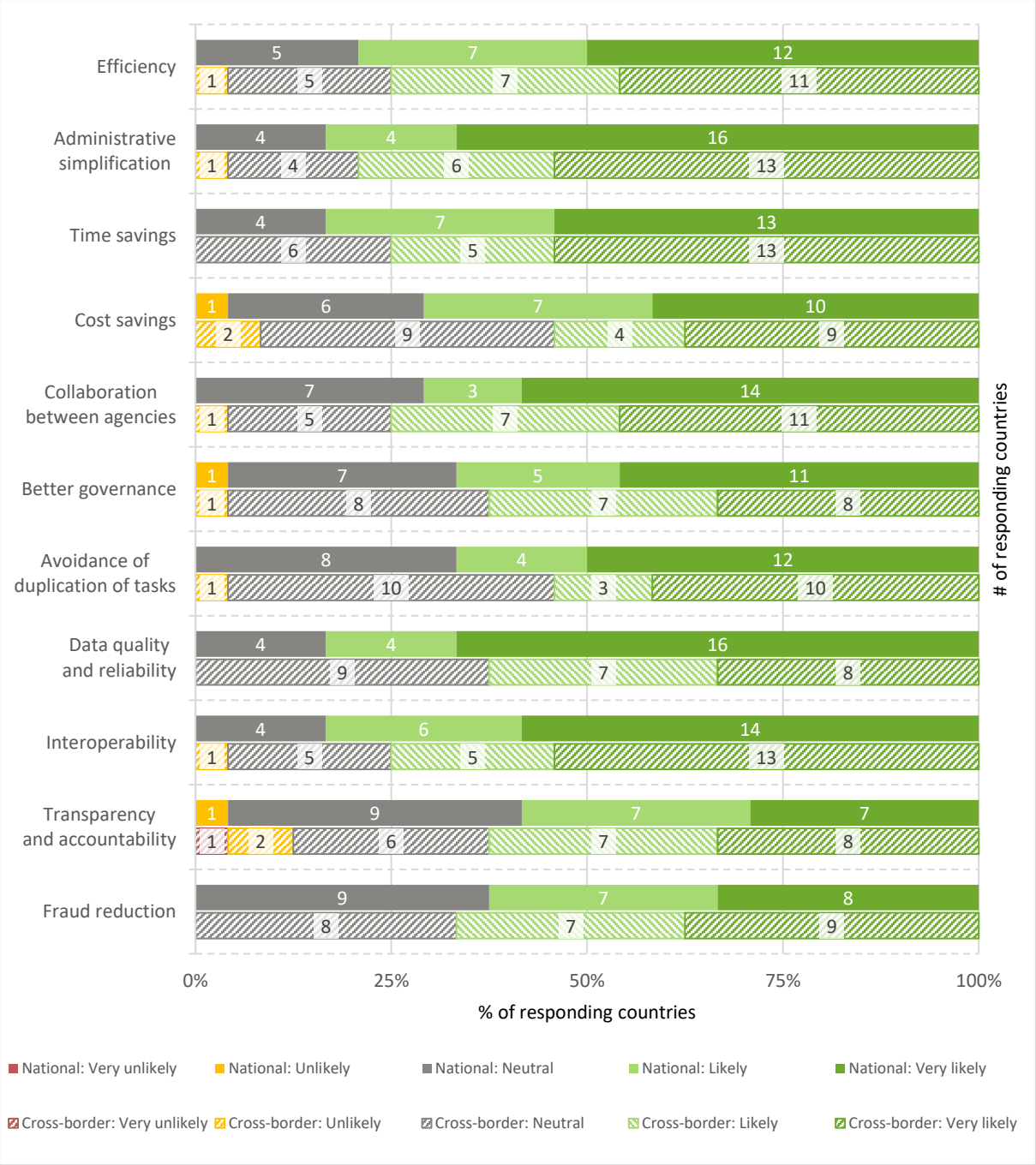

Figure 3 National and cross-border beneficial outcomes of OOP implementation

Responses for unlikely and especially very unlikely are kept to a minimum and only account for just one to two respondents of the respective outcome. Only one country assesses transparency and accountability for being a very unlikely OOP implementation cross-border outcome.

Considering a national perspective, four factors are equally the most likely benefits: Administrative simplification, Time savings, Data quality and reliability, and Interoperability. A total of twenty countries, corresponding to more than 80 percent, find them as a likely or very likely national outcome.

Conversely, the respondents consider the outcome of increased transparency and accountability to be least likely, with only seven countries finding it very likely and seven countries likely. This is followed closely by fraud reduction, which is found very likely by eight and likely by seven. Nonetheless, both

garner approximately 60 percent support. Regarding negative reviews, an impressive eight of the eleven factors have not received a single unlikely or very unlikely outlook.

As in a national context, the overall picture shows a very high expectancy of perceived benefits of OOP in a cross-border context. As such, 50 percent or more of the respondents' regard all of the factors to be likely or very likely. Some reach even more than 70 percent likelihood. Administrative simplification, time savings and interoperability are even regarded to be very likely by 50 percent or more of the respondents.

Regarding negative reviews, three of the eleven factors have not received a single negative outlook on the benefits of implementing OOP. Although this shows that respondents' expectations for cross-border implementation of OOP are lower than that of national implementation, negative reviews are nonetheless still surprisingly few, and as such only add to the overall picture of an overwhelmingly positive estimation of the benefits of implementing OOP.

Comparing the reviews of national and cross-border implementation, national benefits are viewed to be more likely than cross-border benefits for all but transparency and accountability, and fraud reduction. Furthermore, though still receiving an overall favourable rating, the benefits cost savings, and data quality and reliability have the largest differences between the ratings of national and cross-border benefits. Interestingly to notice is that more than 70 percent of the respondents, accounting for 16 countries, expect data quality and reliability to improve significantly on a national level, whereas that just around 30 percent, accounting for 8 respondents, expect improvements in a cross-border context.

3.4 Barriers on Once Only

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 to impede on the European OOP implementation for the respective national governments might provide and indicate some understanding of contemporary implementation levels.

Figure 4 below outlines the respondents' view on the barriers to cross-border implementation. The chart is divided into two sections representing technical and administrative barriers. The latter is further divided into subsections of legal, organisational, economic and political barriers.

As expected, Figure 4 shows that there are quite some barriers affecting the implementation of the OOP. All factors are to some degree considered a moderate, substantial or extreme barrier by the responding countries. 14 of the 17 barriers are even considered "substantial" or "extreme" barriers by 50 percent or more of the respondents. Considering the technical factors, the barriers seem to be more acceptable, as at least two and up to four respondents consider them not as a barrier. Only around 25 percent of the respondents consider them only moderate barriers. Yet still around 50 percent report the technical factors as substantial or extreme barriers.

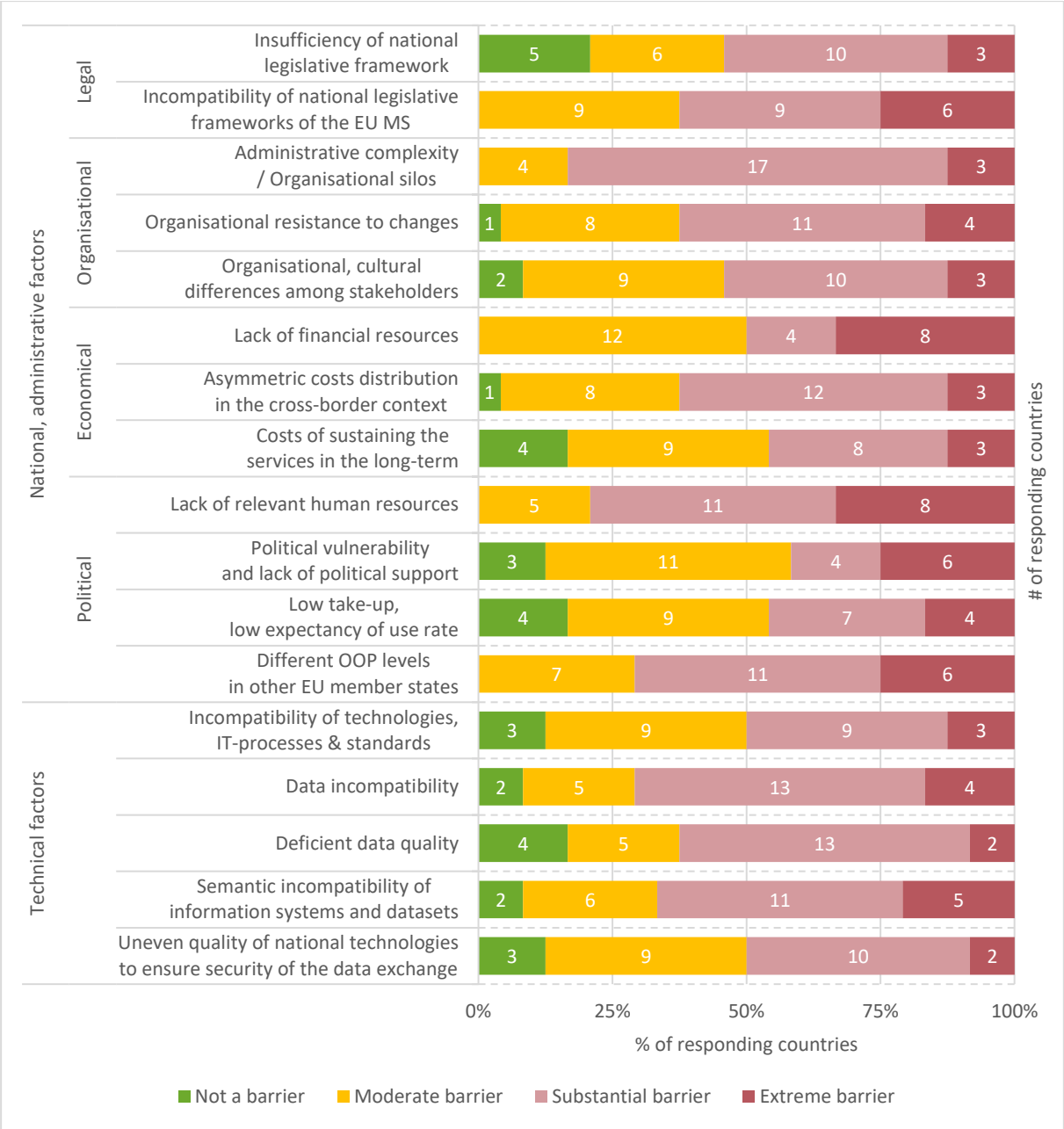

Figure 4 Barriers on OOP implementation

Applying the same views on the barriers as the benefits, 50 percent or more of the respondents consider thirteen of the seventeen factors to be either a substantial or an extreme barrier to implementation of the OOP across-borders. Of these eleven factors, two factors are considered a substantial or an extreme barrier by 75 percent of the respondents.

It seems that the lack of financial and relevant human resources are the two most difficult to overcome. All of the responding countries perceive them as being a barrier and around 30 percent, accounting for eight countries, even as an extreme barrier.

Conversely, the barriers found to be the easiest to overcome are difficult to determine. Nearly 25 percent of the respondents indicate the insufficiency of national legislative frameworks as not being a barrier. On the other hand, more than half of the respondents report the cost of sustaining the services, political vulnerability and a low take-up as a moderate or not a barrier at all.

Interestingly, perception of lack of financial resources appears to divide the respondents. On one side, eight respondents consider it an extreme barrier, which is the highest number of extremely negative reviews. On the other side, twelve respondents only consider it a moderate barrier, leaving four respondents considering it the middle choice, a substantial barrier. A possible explanation could be that the countries have different financial resources available.

A key takeaway, one could argue, is that all factors are perceived as barriers to one extent or the other by the responding countries. However, there seems to be room for discussion as to which is the most substantial one, as they are all equally distributed to some extent. The perceived degree of the barrier depends thus most likely on the level of digitalisation of the respective European administration.

3.5 Willingness to share data

In the DE4A survey, the MS were also asked about their evaluation of the general attitude and willingness towards sharing data in their respective country towards different aspects of OOP[2]. The dotted chart in Figure 5 below shows an aggregated average of the responding countries' willingness to share data with public and private organisations. The chart depicts a somewhat negative observation of a mostly cautious attitude towards different aspects of the OOP. Especially when it comes to sharing personal data with other countries and private organisations within the country, the responding countries report on average a very cautious attitude. Only the willingness to share data with public organisations within the country receives an average score higher than neutral. It is not so high though that it may be interpreted as a positive and open attitude towards sharing data. As such, the analysis documents a general cautiousness among the responding countries towards sharing data.

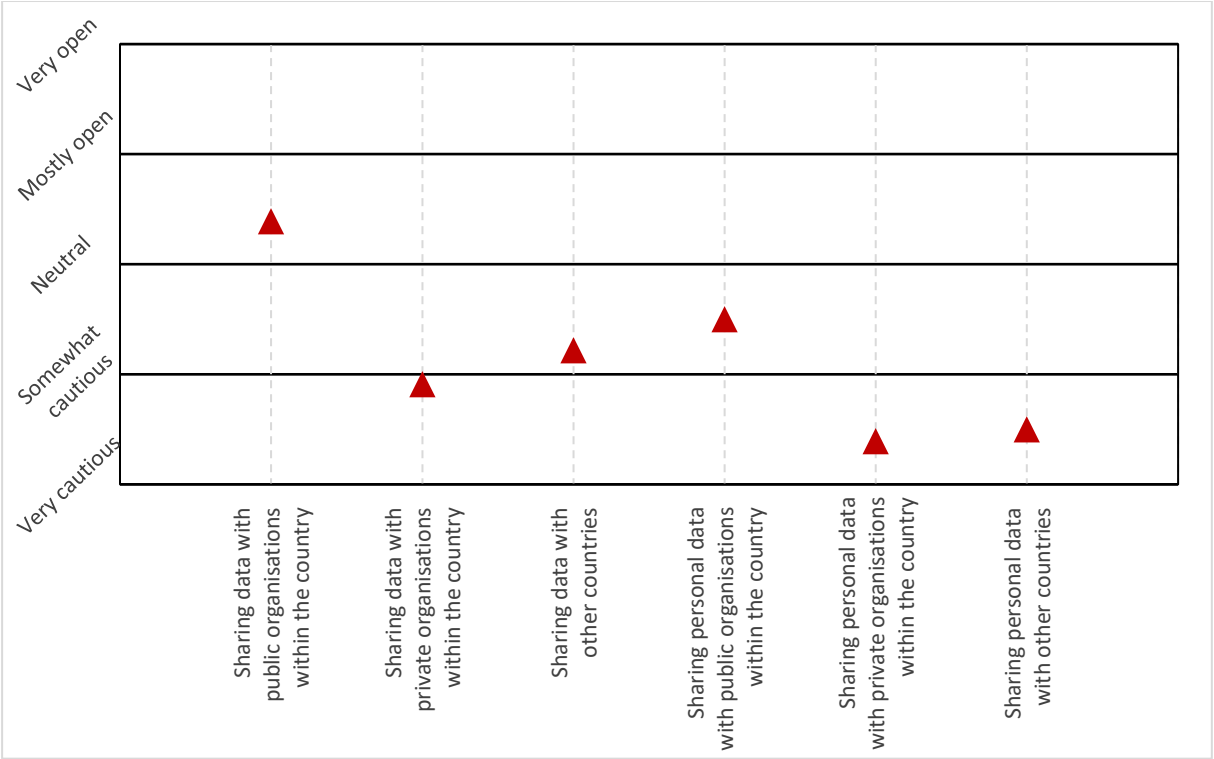

Figure 5 Average willingness to share data with public and private organisations

[2] See question 51 in Annex II. Digital Europe for All (DE4A) survey

Even though the average willingness to share data is somewhat to very cautious among the respondents, a more positive trend can be observed when isolating the responding countries. A more detailed overview of the different answers is illustrated in Figure 6, which shows the willingness to share data in absolute numbers. The attitude towards sharing data with public organisations within the country is mostly to very open for 15 responding countries, accounting for more than 50 percent of all answers. Although considering personal data, only eight countries report a somewhat open attitude, accounting for just over 25 percent, when it comes to sharing personal data with public organisations. On all other aspects, at least 75 percent of the responding countries have very cautious attitude towards sharing data. This is especially visible when it comes to private organisations and sharing personal data.

Considering cross-border, only 25 percent of the respondents report a somewhat open attitude towards sharing data with other countries. However, sharing personal data cross-border is another story, as only two countries, equalling 8 percent, are open towards it.

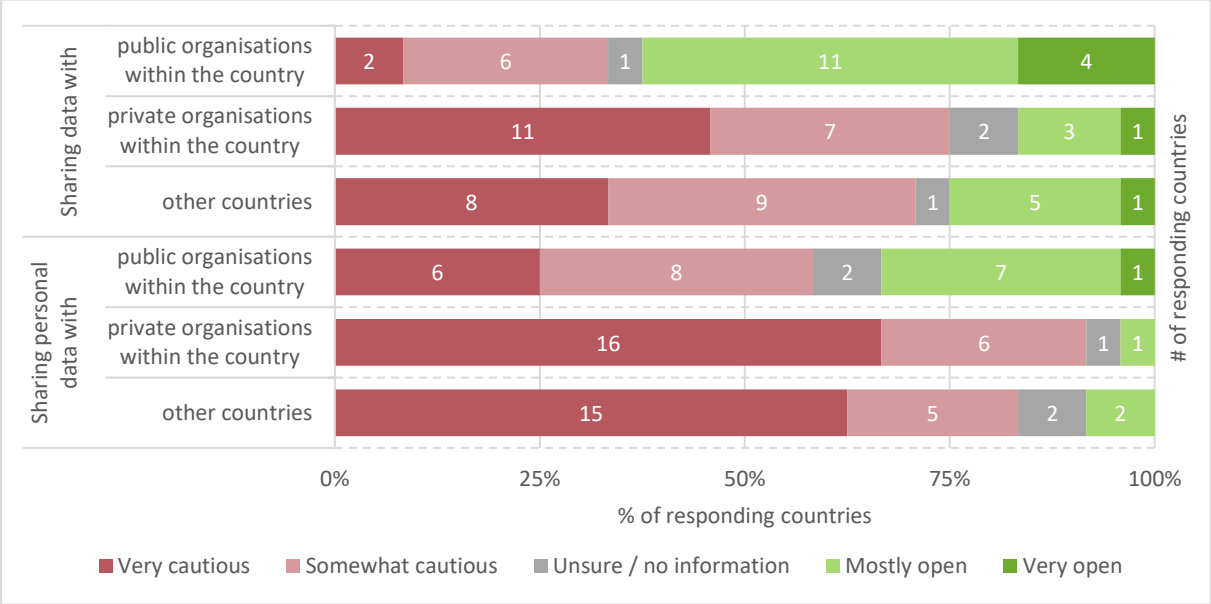

Figure 6 Willingness to share data with public and private organisations

As the total volume of anticipated operations may be expected to have an influence on the perceived value of changes that support cross-border exchange of data, it is interesting to look at the sizes of the populations the responding countries represent. Hence, where the responses in Figure 6 are reported on the level of country, Figure 7 below presents the same responses weighed by the size of the countries' populations. That view on the data underlines the previous observations even more: The countries that are mostly open to sharing personal data with other countries merely represent five percent of the total population of the responding countries. Regarding sharing data with private organisations, the countries that are mostly open represent only three percent of the total population.

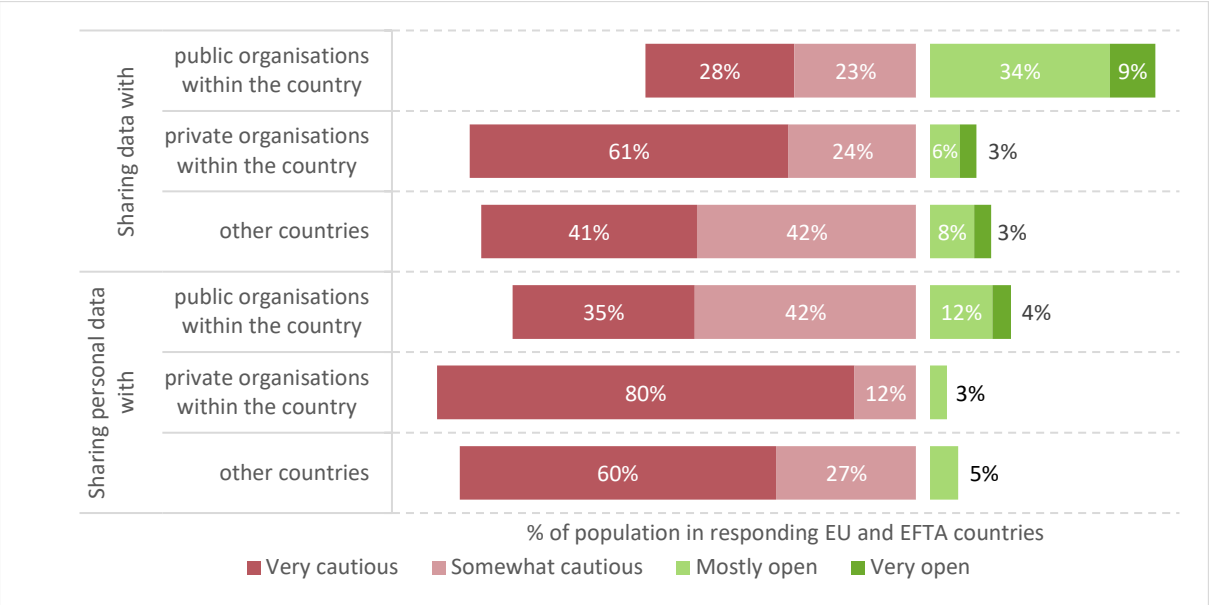

Figure 7 Willingness to share data by EU and EFTA population

In a cross-border context, countries representing a staggering 83 percent of the population report having some degree of caution in regards to sharing data with other countries. When looking at sharing personal data with other countries, even more are cautious, as countries representing 87 percent of the population report some degree of cautiousness. Furthermore, within that group, there is a marked shift towards being very cautious, as countries representing 60 percent of the population report being very cautious towards sharing personal data with other countries.

The data clearly shows a substantial cultural barrier on the implementation of OOP.

3.6 Willingness to change organisational structures

Besides the willingness towards sharing data, the survey also questioned the MS' attitude towards changing organisational structures and technological solutions to enable OOP nationally and cross-border, as there are organisational aspects to most digitisation efforts. The organisational aspects include processes, procedures and structures whilst the technological solutions refer to information systems, architectures, etc.

As with the data presented in the previous section, it can be observed that the corresponding MS are somewhat cautious towards change. Figure 8 maps out the average attitude of the responding MS regarding changing existing organisational structures and technical solutions. Although quite closely aligned, it shows that the responding countries are more cautious in a cross-border than in a national context in regards to OOP implementation.

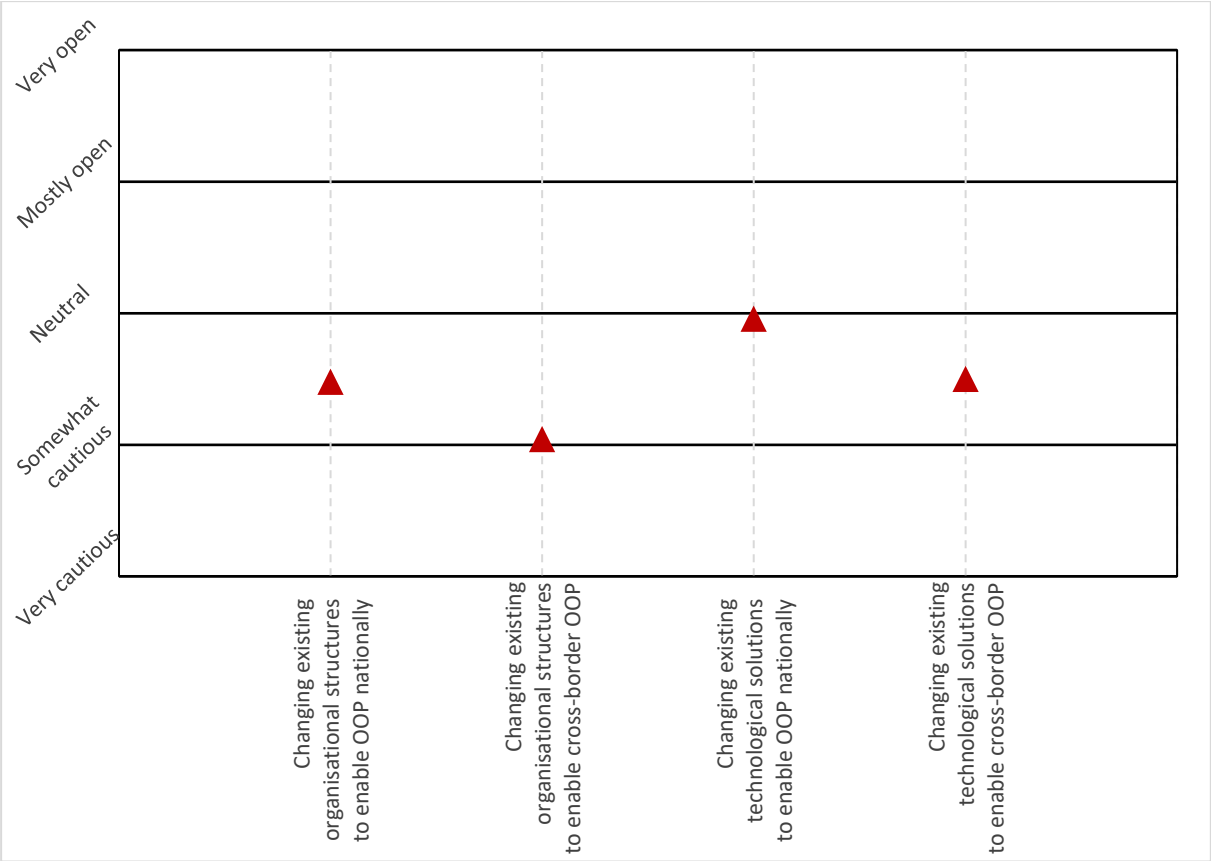

Figure 8 Average willingness to change organisational structures and technological solutions

In a more in-depth depiction of the data, Figure 9 below illustrates that in general only slightly above 25 percent of the responding countries are open towards change. There seems to be a less reluctant attitude towards changing technological solutions, albeit only by a small margin. However, the biggest obstacle in this context appears to be that the responding countries also report being reluctant to change their organisational structures or technical solutions to enable OOP nationally. More than half report a somewhat to very cautious willingness to change.

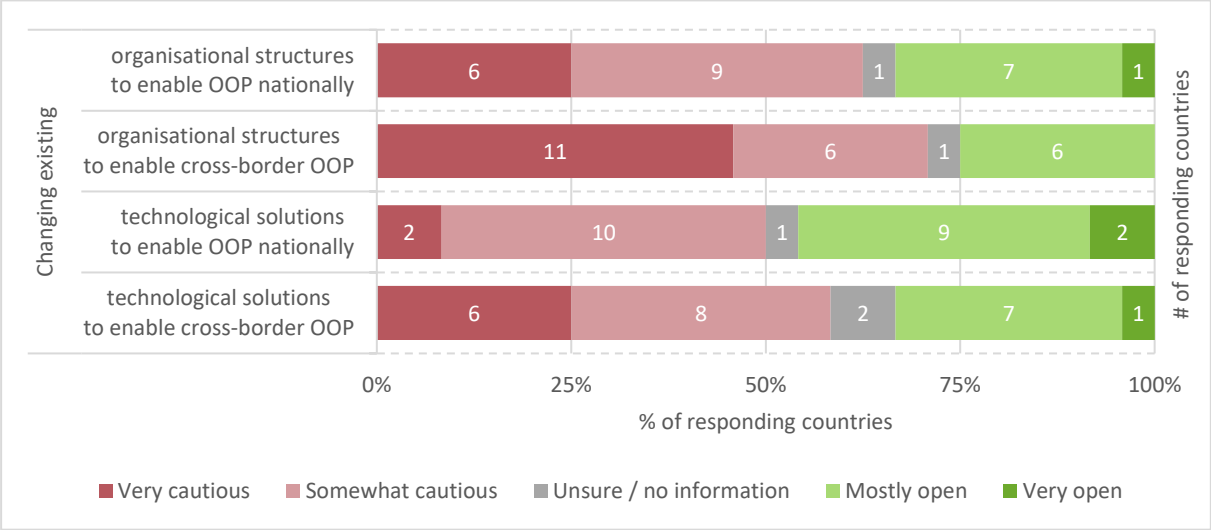

Figure 9 Willingness to change organisational structures and technological solutions

The data presented in this and previous section present a clear cultural barrier on the implementation of OOP. Both in terms of number of countries and in terms of the populations the countries represent, the MS report a very to somewhat cautious picture towards the implementation of OOP. As a cornerstone of cross-border digital services, such a substantial barrier on OOP implies an equally substantial barrier on barrier on integrated cross-border public services as outlined in the Single Digital Gateway.

3.7 National legislation governing Once Only

The previous section presented a very cautious attitude and willingness of European countries towards sharing data as well as changing organisational structures and technological solutions. A different view on the prospects of implementing OOP is given by examining to which extent regulation governing OOP is in place in the MS.

Interestingly, Figure 10 below shows that only two of the responding countries, meaning only 8 percent, do not have specific national legislation governing OOP in place. All other responding countries, 88 percent, report having legislation in place in one way or the other.

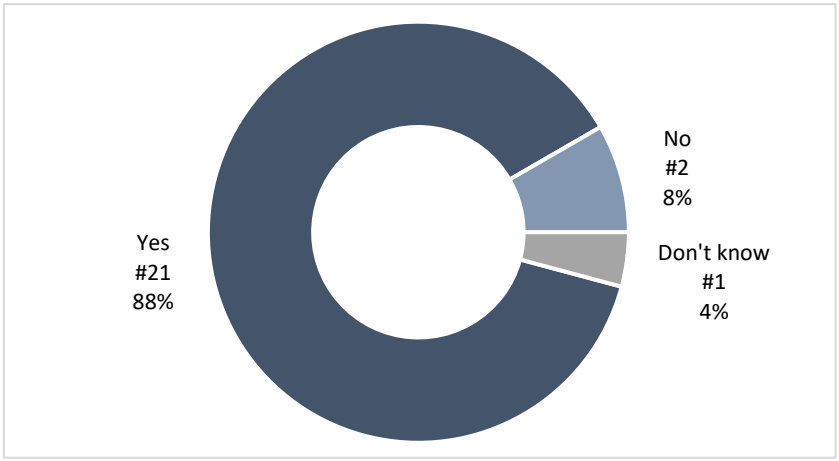

Figure 10 Specific national legislation governing OOP

The key in this context is, however, the phrase specific. The data in Figure 10 refers to specific 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. The political systems of the MS differ significantly from each other. For example, legislation that governs the OOP is in some countries managed nationally whilst on a federal level in others, and thus may create varying regional legislation within the same country. Furthermore, the raw data from the survey shows that the respective legislation in place in some cases only covers marginal sources of data (e.g. databases and registers).

This fragmentation is further observed in Figure 11 below, which illustrates the different procedural or preconditions for an exchange under the said national legislation. Besides some technical and organisational requirements, it becomes clear that regulative factors need to be in place in order to exchange data. Even those countries that reported no conditions for data exchange, also reported authorisation as a legal precondition.

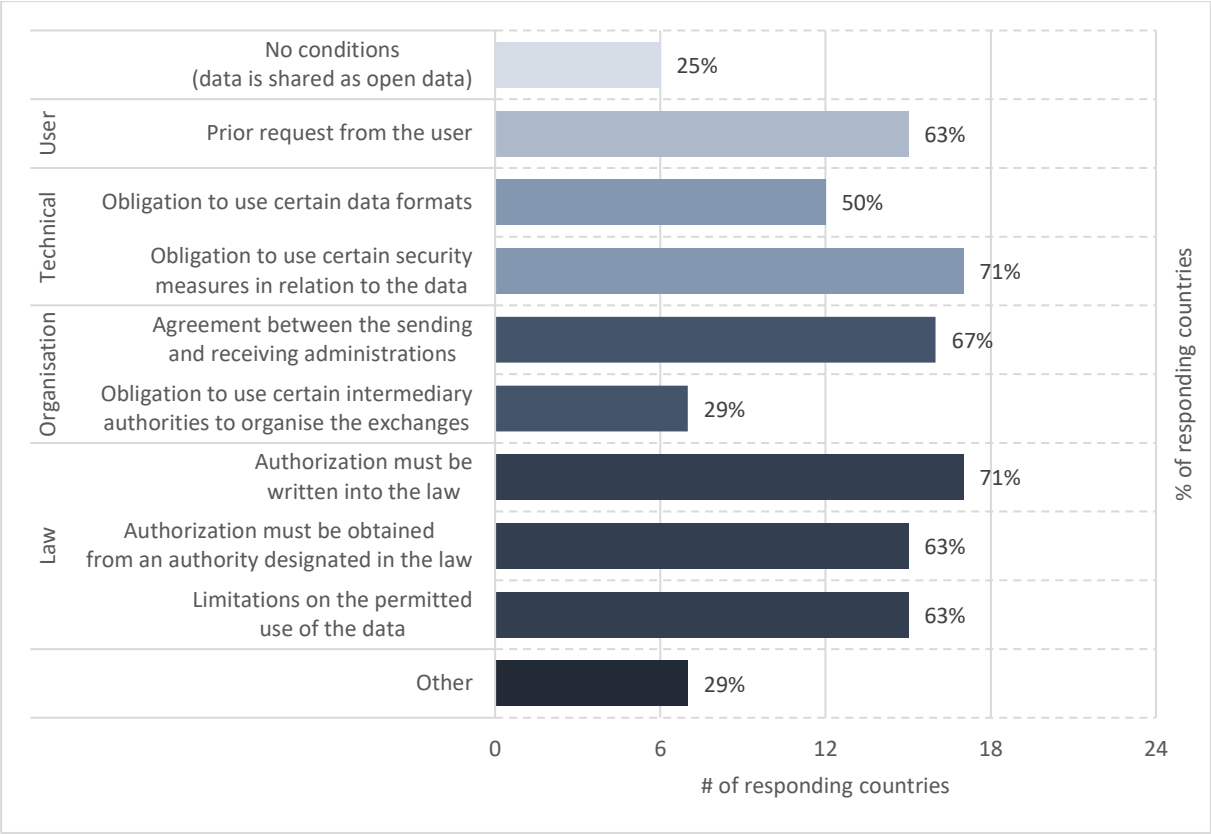

Figure 11 Procedural requirements and preconditions for data exchange

The data shows that legislation is a clear prerequisite for data exchange and therefore a legal barrier necessary to address. National law is a quite 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 made 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 qualitative answers are quantified in Figure 12 and show a quite interesting distribution. Whilst a quarter of the responding countries don´t see any hindrance in requests from foreign administrations, the majority indicates that the law only covers national administrations to request data for exchange. However, a significant portion is still unclear, whether their national legislation covers foreign requests, due to lack of legal analysis.

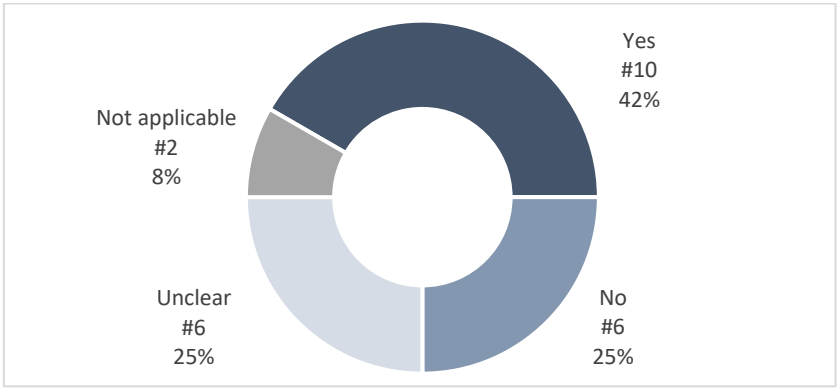

Figure 12 Legal distinction between national and cross-border data requests

When asked about complementary sources for the OOP regulation, three countries, only 13 percent, stated that the national legislation governs the OOP. A quarter of the responding countries indicated the OOP as an unwritten rule or practice. Although most countries have a national legislation in place that covers certain areas of the public sector, more than half report having written guidelines or recommendations as well as non-legislative measures in place.

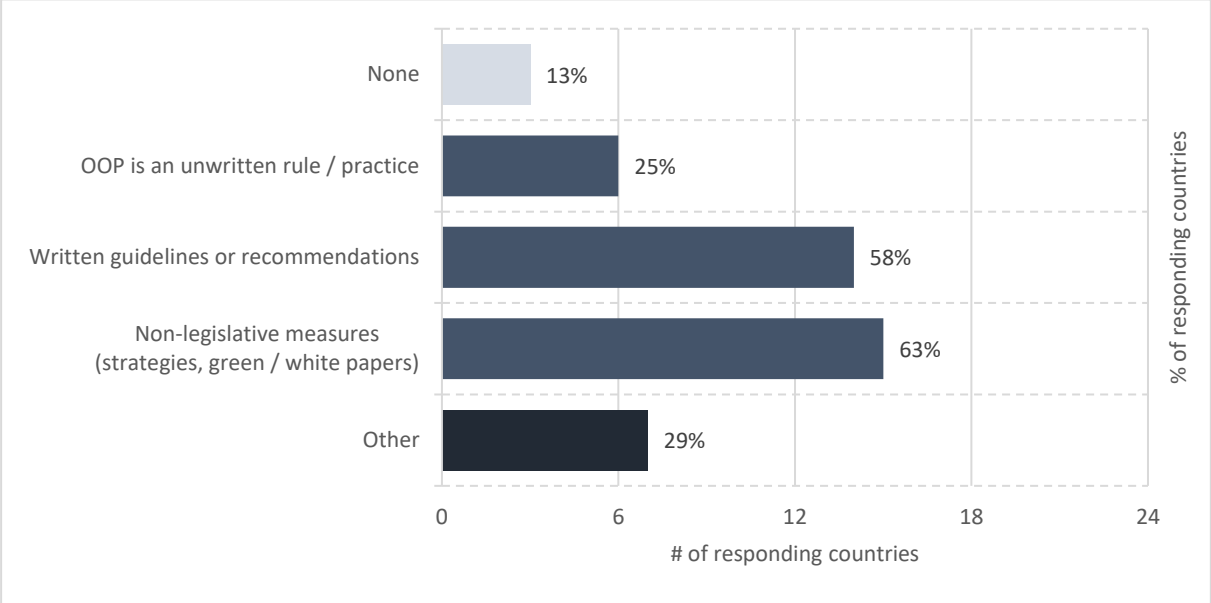

Figure 13 Complementary sources for OOP regulation

Despite there being quite some legal obstacles in place, which probably will take time to be broken down, Figure 13 indicates that a majority of the responding countries already address the OOP nationally with soft-law measures. On the other hand, the data has shown that there is a clear need for the different national laws to be harmonised to enable the SDGR and a successful implementation of the OOP.

4 Risks and barriers

4.1 Legal risks and barriers

This section will list and briefly describe select legal barriers. Several barriers are described in greater detail in the DE4A legal white papers.

The identified barriers have been categorised into four different groups, arranged from generic to specific. Furthermore, to the extent possible, within each category the barriers are listed from most generic to most specific.

4.1.1 Barriers to access to data

L1: Lack of legal basis for exchanging data

Source: Expert Interview, Survey, TOOP and DE4A Pilot

Barrier: Integrated services use a wide array of data in order to provide the best or most accurate service. Prior to any exchange of data between competent authorities, a legal basis for that exchange must be established. In many countries, the basis for exchanging data is provided by law and complemented by data exchange agreements between the sending and each of the receiving authorities. The DE4A survey identified that 71% of the countries stated that authorisation was specified in law, and that 42% indicated that the law only grants access to national authorities. This is typically possible, because the number of relevant authorities per data set is relatively limited. Despite being EU regulation, it is not given that the SDGR in itself provides the legal basis for the cross-border exchange of data. As such, any cross-border exchange of data will need to use the same legal basis at current national exchanges of data.

However, those mechanisms are not operational in a cross-border context, as the number of relevant authorities grows exponentially and changes more often.

If use of consent is not adequate for overcoming this barrier, an enabler could be to add to national legislation “competent EU-EFTA authorities” as legitimate users of data. However, in order to work with the broader term “competent authority”, rather than a more narrow term like “peer”. Such a solution would require organisational, semantic and technical enablers, as the number of potentially competent authorities would otherwise still be unmanageable for each data providing authority. If supported by a system of federated trust between MS, whereby e.g. national nodes attest to the identity and competence, of any given national authority under its jurisdiction, including its legal grounds for requesting data. This would drastically limit the number of entities any given authority would have to manage.

A variant of the barrier lack of legal grounds for exchanging data is the barrier legal provisions specifically hindering (cross-border) exchange of data.

Issues of data protection, that the data responsible authority may not overlook, causes barriers to the user-centric design and process simplification. That hinders demand, resulting in poor return of investment (ROI) on service development.

Driver: Focus on areas where legal ground for cross border exchange exists and legal clarification regarding applicability of user consent. Continued focus on European legal policies for sharing of personal data between public authorities and relevant use cases.

4.1.2 Barriers derived from non-equivalence of national law

L2: National law constitutes a barrier on cross-border demand for services

Source: TOOP and DE4A Pilot

Barrier: Although the Single Market has been a cornerstone of the European cooperation for decades, its implications on especially member states' social benefits is often the focus of the public and political debate. Consequentially, in some cases, national law specifically hinders access to various types of services by installing eligibility criteria that are not directly bound to nationality but nonetheless hinders mobility, e.g. residency, employment and so forth.

Drivers and enablers: Focus on services with a positive ROI, national or cross-border.

4.1.3 Barriers on Cross-border reuse of data as is

L3 Requirements for translation of data/evidences

Source: Expert Interview

Barrier: For any competent authority, understanding the meaning of a piece of evidence is evidently of great importance for assessing its bearing on a case. To avoid spending vast resources translating evidence, most European countries have services where evidences may only be submitted in a few languages. Furthermore, any translation of the original evidence may also be required to be attested or apostilled.

Such a requirement, for submitting evidence in specific languages, imposes a barrier on the exchange of data between competent authorities based on a user's request, as the data providing authority in most cases will only have the evidence in that MS' official language. Such a requirement then effectively puts the process on a halt, and forces the user to resubmit manually after having the evidence translated. Other aspects of this barrier, e.g. different countries' use of different legal terms for the same object or conversely using the same term for different objects, are discussed in the sections on semantic barriers.

Enabler: Development and/or implementation of standardised evidence for commonly used types of evidence, e.g. base registry data like person, cadastre, and company information. This may either enable the issuing of evidence in the requested language, or by adhering to common semantic standards. The receiving authority may no longer need to know the meaning of each term in a certificate. Other examples of enablers could be the use of common vocabularies, ontologies and code or authoritative lists, multilingual labels and values, and culture-agnostic precise definitions. Besides, an agreement/regulation is needed for the recognition of these measures among MS. Reusing already existing sectoral agreement on this regard is a good starting point.

L4: National requirements for original and /or certified copies of evidence.

Source: DE4A Pilot

Barriers: Equally as evident as understanding the content of a piece of evidence, is trusting that its content is correct. Historically, this trust has been based on a requirement for original and/or certified copies of the evidence. Now, as processes become more digitised, validating the content of evidence is done more easily and with a higher level of assurance by use of electronic trust services, like electronic signatures. Despite the benefits, the shift to reliance on electronic signature and electronic seals has still not taken place, requirements for original and/or certified copies of evidence are still prevalent, and acceptance of electronically attested evidence, or data from a registry, is still not the norm.

Enabler: Legal steps like obliging the acceptance of electronic attestation or equating a data registry response with a certificate would shift the balance away from use of originals. However, as the barrier is rooted in organisational resistance to change, and has organisational implications, a soft-power approach, like communicating the financial and security benefits of shifting away from relying on originals, could be equally effective.

L5: Lack of recognition of value and trust in electronic signatures by public administrations

Source: Expert Interview

Barrier: The legal value of eSignatures lacks recognition and the legal requirements on signers are not always clear. Adoption of eSignature types such as eSeals to sign "data transmission / exchanged data" is low especially in cross border context. This barrier has technical implications.

Driver: Regulation for Public Administrations to accept the legal value of digital means

L6: Complex legal processes such as requirement for central validation of documents/evidences

Source: DE4A Pilot

Barrier: Processes for accepting documents/evidences are not designed for efficient, decentralised interaction, but may require centralized approval. The barrier also has organisational implications.

Driver: Increased reliance on cross-border trust services such as electronic signature and electronic seal to verify validity of documents/evidences

4.1.4 Barriers on secure User Identity Management

L7: Challenge to manage User Consent transitivity across borders between authorities.

Source: Expert Interview

Barrier: Consent is often given by the user as part of an online procedure provided by a public entity in one country. The validity and scope of the consent need to the transferred to the data provider in another country. User consents and their exchange should be traceable and auditable. If the data provider cannot verify the user consent, it may be a barrier to data exchange.

Driver: For the exchange of personal data, the proof of the user consent should be sharable under non-repudiation conditions, i.e., users could not deny that such consent was given by them. Besides, a trusted model should be put in place for the exchange of information between Once-Only Technical System (OOTS) nodes in the same way as the eIDAS nodes.

L8: Identity transitivity cross border

Source: Expert Interview

Barrier: In order to ensure compliance with information security regulation, including GDPR, a data provider must have adequate assurance of the identity of a user prior to revealing e.g. personal data. In a cross-border context, the user identity is established by the public entity providing an online procedure by means of eIDAS attributes. When requesting data related to the specific user, the Identity of the user needs to be transferred to the data provider. If the data provider cannot verify the user identity by those same means, it may be a barrier on data exchange as questions arise of how to properly establish the identity of the user at the data provider, and at the same time ensure that it is the same or an equivalent identity that is provided to the data consumer. If the user does not have a persistent identifier linked to her eID, this issue is further complicated by time, as electronic identification change, thus severing ties to the identity, the data provider has stored the evidence under.

The barrier has technical implications.

Enabler: Extension of minimum eIDAS attributes to any and all simultaneous and historic eIDAS identifiers.

L9: Challenge to reuse the User Consent

Source: Expert Interview

Barrier: Challenge to reuse the User Consent for recurrent stand-alone renovation of the status given to the user after the first application (e.g., pensions renewal that requires a new request for the user's annual incomes)

Enabler: Ensure legal basis for reuse of consent implemented by development of standardised notification mechanisms with option for the revocation of the given user consent.

L10: Revocation of User Consent.

Source: Expert Interview

Barrier: Competent authorities of online procedures should keep the given user consents while the corresponding data treatment is in place. They also need to allow users to check their active user consents and to revoke them.

Enabler: Ensure legal basis for implementation supporting auditing and easy access for user to revoke consent.

4.2 Organisational risks and barriers

O1: Data may be not ready for access in real-time without authorisation by a civil servant

Source: Expert Interview

Barrier: In some MS and use cases data does not have a legal value unless the evidence is authorised by a civil servant involving a manual procedure. In some cases it is related to legacy procedures and partial digitisation of data or it can be a result of legal provisions in the country. This barrier may cause a delay in transfer of evidences. The barrier also has legal aspects.

Driver: For procedures capable of a waiting-for-evidence status, the user can be informed of the possibility of collecting some evidences automatically after finishing the online session or providing such evidences by their own in a new session from the scratch. If the first option is chosen by the user, the procedure could end with a receipt with a reference number and a brief explanation of waiting-for-evidence status. Besides such interrupted procedures, focus on implementation of policies could ensure legal value of data retrieved from authoritative data sources.

O2: Data may not be ready for access in real-time without following procedures involving batch processing

Source: Expert Interview

Barrier: Due to legacy, systems designed for operations scheduled according to administrative processes and user patterns originated before digital internet online self-service portals with 24/7 access became common, access to data may be subject to batch processing procedures. The required transformation is similar to transformation in the financial sector when internet-banking solutions made banking services such as money transfer available to users online. This barrier may result in delayed transfer of evidences.

Driver: The digital transformation is required to support user-centric designed online procedures with the quick response. Drivers include improved user satisfaction with possibility to increase number of self-service transactions as well as better reuse of data

O3: Access to data may be subject to charges

Source: Expert Interview, DE4A Pilot, Survey and TOOP

Barrier: In some cases, access to data by public authorities requires payment of fee to the data provider. National payment schemed to facilitate transfer of funds between authorities based on number of transactions seems cumbersome and expensive in the cross-border context. As such, collection of evidence is often done in other ways.

The barrier also has legal and technical aspects.

Driver: The barrier may be addressed by alternative mitigating efforts:

- Pre-payment of the exchange by the user before starting the procedure. This should be explicitly and clearly explained in the instructions of the procedure. The user should provide the reference of the payment issued by the DP, in order to include it in the DC request.
- Implementations involving user redirection to the DP payment can be handled directly by the user after the data is accepted in a preview process, before the data is sent to the DC.
- The effort to increase the datasets free of charge, such as OpenData, may be extended to cover cross-border access to data relevant for public services. This could increase the reuse of data and the value for users.

O4: SDG User preview at data provider may be a barrier for a coherent user journey

Source: Expert Interview

Barrier: This issue has also legal implications as the preview function is described and required by SDGR. SDG preview of data/evidence by user is defined to take place before data/evidence is sent to data-consuming services provider. This can be a barrier for coherent user-journey and require new user interface services by data providers.

Driver: A four corner design for the exchange would consider data evaluators/requestors as DC and data owners/transferors as DP. Data owners are the authorities responsible of the data and data evaluators are data consuming authorities, so both types of actor are component authorities. However, data requestors/transferors can be seen as part of the OOTS. In consequence, if data requestors handle the preview, it is happening before the data consuming authority has received the data. In this sense, user journeys can be handled in a coherent way by only one MS.

O5: Integrated Public Service Governance - How authorities address their counterparts in other MS.

Source: Expert Interview, TOOP

Barrier: In order to send a request for data to a competent authority in different MS, it is required that there is a defined way to find and address the receiver of the request. This involves identification of data sources describing available types of evidences and where they are located.

Enabler: At least a directory of data controllers for every competent authority involved in the integrated provision of public services should be available. TOOP is piloting this approach and the solution is expected to be valuable for future use. Various sectoral collaborative networks already have this kind of directories, for instance Internal Market Information systems.

O6: Integrated Public Service Governance - availability, quality, required functionality of central building blocks and connection hubs of MSs.

Source: Expert Interview and TOOP

Barrier: This barrier includes the organisational aspects of implementing a data-sharing infrastructure supporting Once Only and integrated public services including service level agreements etc.

Driver: Design and implementation of governance structures that can support implementation and lifecycle management of required components and services. Further detailed requirements of specifications for interfaces and processes are required.

O7: Integrated Public Service Governance - Auditing and Traceability (supporting transparency, problem solving, detecting cause of malfunctions)

Source: Expert Interview

Barrier: This barrier includes the organisational aspects of implementing a data-sharing infrastructure supporting Once Only and integrated public services, is areas such as common standards and procedures for logging, support services access and problem solving.

Enabler: Common guidelines for collecting and keeping traces and audit logs to allow the transparency, traceability and auditability of the data exchanges. This information should be also interoperable in order to collaborate among MSs in these tasks.

O8: Different levels of data quality and other data constraints.

Source: Expert Interview

Barrier: Different levels of data quality and other data constraints may require modification/differentiation of services processes and required data/evidences

Enabler: Vocabularies that allow the description of data quality and data availability constraints regarding the evidences lawfully issued by the different competent authorities. If DC considers that the informed data quality or data constraints prevent from the use of the OOTS, it can inform users to provide the evidence by their own. The preview functionality is also a measure for mitigating the data quality.

O9: Different systems for distribution of regulatory responsibility in MSs can complicate finding right authority.

Source: Expert Interview

Barrier: Different distributions of regulatory responsibility can make it very difficult to know what is the right competent authority for lawfully issuing an evidence or what information should be required from the user to identify such a competent authority.

Enabler: The evidence broker and data service directory [14] should provide such information to allow the online procedure to ask the user for the information needed for locating the right competent authority for the evidence. This could supplement finding the data provider based on catalogue of datasets/evidence types and defined criteria. However, any such function has to be

O10: Lack of trust (cultural) across member states

Source: Expert Interview, Survey and TOOP

Barrier: There may be an uncertainty of the quality or a limited willingness to recognise the quality of data and validity of evidences/datasets from other MS.

Driver: Defining standards for data quality and procedures for validating data quality may support improved data quality as well as acceptance from other MS.

O11: Different strategies in MSs for implementation of Public services

Source: Expert Interview

Barrier: MSs support the digital transformation towards public services in different ways. This includes levels of centralisation, strategic focus (or lack of strategy) on architectural and other structural aspects of implementations covering national digital infrastructures and processes.

Driver: An increased level of coordinated policy addressing interoperability requirements may improve and make cross border services simpler to implement. This could include increased focus on common architectural frameworks like EIF and alignment of data definitions to European core vocabularies. Further, key digital enablers such as eID, eSignature and reusable infrastructures for secure communication and exchange of data could improve functionality and extended to cover a wider range of use cases.

O12: Low return on investment for public services to be digitised

Source: DE4A Pilot

Barrier: As the public sector in every MS must balance competing political priorities, it may be assumed that initiatives are evaluated against their expected ROI. By extension, an initiative's perceived ROI is likely to decide whether or not that initiative will garner political and organisational support. However, as the initiative must be understood in the context of fiscal priorities, ROI is relative to that of other initiatives – digital or not. This is a natural, but nonetheless major barrier on digitisation efforts.

Furthermore, some sector systems have been implemented reusing generic building blocks such as eDelivery, but due to sectorial governance and differences in implementation such as addressing and security they may not be fit for reuse in other sectors or use cases.

Driver: Focus on identifying initiatives with the highest and most immediate ROI, whilst in the execution thereof ensuring that components support re-use. Focus on cross sector governance and increased re-use of digital infrastructures may reduce costs for implementation and operations.

O13: Issuing and acceptance of electronically signed documents can be a challenge for authorities

Source: DE4A Pilot, survey

Barrier: Although there may be legal grounds to use and accept electronic signatures, there may be organisational and procedural barriers on the practical use of these means. Even if technical solutions are available, these may not be implemented as part of the procedures use by the public entities. This could involve the adoption and management of electronic Signatures and Seals as well as the capabilities to verify validity of received signed datasets and documents. Although eIDAS creates a basis for solutions, it is not yet widely adopted.

Drivers: Focus and recognition of benefits such as improved security when moving to electronic signatures as well as continued work to ease implementation of e-signatures and seals by improving generic cross-border building blocks based on eIDAS.

O14: Low uptake of eID hinders high volume demand for electronic public services, resulting in low ROI

Source: DE4A Pilot

Barrier: High ROI presumes that a significant proportion of users actually use the digital solutions. This often requires strong policy measures, such as legal regulation. Those legal measures may not always be applicable in a European context (e.g. mandatory use of digital services).

Driver: Active cooperation between all levels of government to be a success. Promotion and adoption of policies supporting the process towards "Digital by Default" and "Digital Only" for public services.

O15: Lack of willingness to share data

Source: Survey

Barrier: From a national perspective, many MS public authorities are cautious to share data with other entities. Most MS are even more cautious to share data cross-border, even with public authorities in other countries.

Driver: To mitigate this barrier clear policies and regulation with well-defined objectives can be effective. Furthermore, documentation of results and benefits are needed to mitigate the cultural barriers. In addition to this, initiatives within each MS, where the level of trust is most often the highest, may provide the necessary experience with sharing data, that caution towards cross-border sharing may decline.

4.3 Semantic risks and barriers

S1: Diverse and non-harmonised types of criteria and evidences in different member states can make it difficult to find and request relevant evidences

Source: Expert Interview and DE4A Pilot

Barrier: Lack of equivalence between requirements and credentials in different MSs may lead to difficulties in finding correct evidence to prove a given criteria.

Driver: An evidence broker should provide a functionality to allow the matching between domestic criteria/evidences and common criteria/evidences for locating the right cross-border evidence and to allow the locating of the appropriate data service to retrieve such an evidence (Data Service Directory).

S2: Evidence Format and cross-MS Compatibility of Formats

Source: Expert Interview and TOOP

Barrier: MSs have implemented different digital formats and even different level of digitization of evidences. This can be a barrier to understand and reuse data obtained from other MSs. TOOP is piloting use cases supporting interoperability using harmonised data and mapping of data.

Driver: Agreement on a common data format for structured and non-structured documents. Attach structured harmonised data whenever possible. Results from TOOP can be useful solutions.

S3: Missing Semantic mapping of data elements

Source: Expert Interview

Barrier: Evidences are defined in MSs to be used in a given context. The data elements used in evidences are defined to represent information with a given definition that may be explicitly legally defined or more implicit. In case of re-use of the evidences, the context can change and the interpretation of data elements can be a barrier. An example could be that the value of the annual income for a citizen may be defined differently in different MSs causing a barrier for reuse of such data.

Enabler: Use of canonical forms or common data models that are harmonised can mitigate this barrier. The European Core Vocabularies cover important areas of public services and can be used for mapping data elements.

Driver: National digitisation efforts encounter the same issues, especially when reusing evidence across different legal grounds or different sectors. This may lead to national harmonisation efforts, cross-border efforts may benefit from.

S4: Different levels of data quality may be a barrier on the use of data by cross-border procedures

Source: Expert Interview

Barrier: If available evidences have a low quality or even an uncertain level of quality, it may be necessary to adapt processes to ensure correct results. This is especially a barrier for countries or sectors with a high degree of automated processes.

This barrier also has organisational aspects.

Enabler: A functionality to allow the description of data quality and data constraints of the available evidences issued by the different competent authorities. DC then can use this information to assess the usability of the evidence regarding its data quality and constraints.

S5: Identity/record matching when accessing online services cross-border

Source: Expert Interview

Barrier: Citizens may have several defined registered identities across MSs. In many MSs citizens are assigned a Personal identifier that is used within the country to give a citizen a unique personal identifier (PID) that can link information in different registries and databases securely and uniquely to the specific individual. In many processes, it is required to establish the link between the eIDAS authenticated user and the national PID in order to give access to personal information and execute the procedure. The eIDAS mandatory attributes may not be sufficient to make a secure Identity matching. In some cases, a manual process is necessary to complete the possible automated identity/record matching.

This barrier also has legal aspects.

Driver: DC should handle the identity/record matching as required in their own country and particular situation. Possible extension of eIDAS dataset with more attributes.

S6: Identity/record matching of user for data request and data access

Source: Expert Interview

Barrier: Citizens may have several defined registered identities across MSs. In many MSs citizens are assigned a Personal identifier that is used within the country to give a citizen a unique PID that can link information in different registries and databases securely and uniquely to the specific individual. In many processes, it is required to establish the link between the eIDAS authenticated user and the national PID in order to give access to personal information and execute the procedure.

In cases such as SDG implementation of Once Only it is required to provide data/evidence in “real-time” when the user is engaging in an online procedure. This prevents additional manual on boarding procedures to be applied.

Driver: 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.

S7: Integration with sectoral infrastructures

Source: Expert Interview

Barrier: Existing Integrated cross border services are often supported by sectorial defined infrastructures and services. Integrations between existing sector solutions and new procedures defined by SDGR may be cross sector as well as cross border and require complex integrations to fulfil their purpose. This barrier has implications for the technical Once Only implementation.

Driver: If the procedure belongs to the same sectoral domain, the already in-place semantics can be used, otherwise, a mapping between the sectorial ontology and the domain-agnostic vocabulary used for could help.

S8: Non-harmonised (or mapped) user rights, including powers and mandates

Source: DE4A Pilot and SEMPER

Barrier: eIDAS does not support powers and mandates which have led to diverse solutions (or lack of solutions) in MSs that are not compatible and interoperable across borders. This prevents effective cross-border use case implementations.

Driver: Development and implementation of standards and governance to cater for interoperable "powers and mandates" solutions cross-border – possibly extension of eIDAS to include such provisions.

4.4 Technological risks and barriers

T1: Integration with sectoral infrastructures

Source: Expert Interview and TOOP

Barrier: For cross-sector use cases involving existing infrastructure services and networks for data exchange, implementations may require interoperability with sectoral solutions or duplication of efforts for those actors already connected.

Architectural design, use of different standards and technologies may cause barriers for interoperability. Examples include different addressing schemes, security measures and policies, and governance procedures specific to domain specific sector solutions. These barriers lead to increased costs when connecting to domain/sector solutions.

Driver: 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.

T2: Integration with national infrastructures

Source: Expert Interview

Barrier: All cross border infrastructures need to be integrated with national solutions to achieve interoperability and coherent user journeys. Examples include routing to authorities, data access and integration of services with eID, eSignature and access management controls.

Driver: Implementation of standardised 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.

T3: The managing and governance of the choreography of distributed components managed by different agents and during a single user session

Source: Expert Interview

Barrier: It may be difficult to implement robust processes and user journeys supporting use cases involving components, gateways and services from two or more MSs in addition to central services such as registries and mapping services.

Driver: Develop architectures with clear division of responsibility and simple transparent interfaces. Consistent use of standards to opening markets for commercial technology, platforms and implementations can also be a driver for improving availability of production grade solutions.

T4: Synchronicity of data exchanges

Source: Expert Interview

Barrier: Some services and national solutions cannot provide "real-time data". The digital transformation with shift towards online internet-based services and 24/7 access are placing new requirements on platforms, databases and systems implementing public services.

Driver: Investments in new technology and platforms including portal solutions for public services provisions may actually cut costs for operations and lower resources required support for non-digital channels and services.

T5: Current eID minimum data set only offers identity for specific point in time

Source: DE4A Pilot

Barrier: The present implementations of electronic identity schemes are not properly linked to historic and/or persistent identity.

This barrier appears to be of a technical nature, but it also has legal, organisational and semantic aspects. It is especially a barrier for cases spanning over several years, such as pensions, retrieving old diplomas and more.

Driver: Extension of eIDAS eID with improved temporal management support.

4.5 Inventory of existing risks and barriers

Table 2 Inventory of legal risks and barriers

#	Identified risk or barrier	Probability 1-5	Consequence 1-5	Total score 1-25	Potential drivers and enablers
L1	Lack of legal basis for exchanging data	4	5	20	SDGR, GDPR, eIDAS, federated registry of authorities' competences
L2	National law constitutes a barrier on cross-border demand for services	2	2	4	Focus on services with a positive return on investment, national or cross-border.
L3	Requirements for legal translation of data/evidences	3	5	15	Development and/or implementation of standardised evidence
L4	National requirements for original and /or certified copies of evidence	4	3	12	Focus on legal policies to accept digital evidences
L5	Lack of recognition of value and trust in electronic signatures	3	5	15	Regulation for public administrations to accept the legal value of digital
L6	Complex legal processes such as requirement for central validation of documents/evidences	2	3	6	Rely on cross-border trust services such as electronic signature and electronic seal to verify validity of documents/evidences
L7	Challenge to manage User Consent transitivity cross-borders between authorities	5	4	20	Semantic standardisation of consent, technical solution to transfer (proof of) consent, based on eIDAS framework
L8	Identity transitivity cross-border	5	5	25	Implementation of standards-based solution based on eIDAS framework
L9	Challenge to reuse the User Consent	4	2	8	Ensure legal basis for reuse of consent implemented by development of standardised notification mechanisms with option for the revocation of the given user consent
L10	Revocation of User Consent	2	2	4	Ensure legal basis for with implementation supporting auditing and easy access for user to revoke consent.

Table 3 Inventory of organisational risks and barriers

#	Identified risk or barrier	Probability 1-5	Consequence 1-5	Total score 1-25	Potential drivers and enablers
O1	Data may be not ready for access in real-time without authorisation	4	3	12	Implementation of interrupted procedure. Take steps to ensure legal value of data retrieved from authoritative data sources.
O2	Data may not be ready for access in real-time without following procedures involving batch processing	3	3	9	Technical solutions for in-waiting processes. Take steps to update solution architectures.
O3	Data may be subject to charges	3	5	15	Implement prepayment system. Redirection of user session to Data provider for payment. Reduce cross border payment for public data.
O4	SDG User preview at data provider may be a barrier for a coherent user journey	4	4	16	Four-corner model for data exchange and preview implemented by Data requester/transferor
O5	Integrated Public Service Governance - How authorities address their counterparts in other MS	3	5	15	Directory of data controllers for every competent authority involve in the integrated provision of public services should be available.
O6	Integrated Public Service Governance - availability, quality, required functionality of centrals building blocks and connection hubs of MSs	4	4	16	Design and implementation of governance structures that can support implementation and lifecycle management of required components and services. Further detailed requirements of specifications for interfaces and processes are required.
O7	Integrated Public Service Governance - Auditing and Traceability (supporting transparency, problem solving, detecting cause of malfunctions)	4	4	16	There is a need of common guidelines for collecting and keeping traces and audit logs to allow the transparency, traceability and auditability of the data exchanges. This information should be also interoperable in order to collaborate among MSs in these tasks.
O8	Different levels of data quality and other data constraints.	4	5	20	Measures and standards to manage and monitor data quality.

#	Identified risk or barrier	Probability 1-5	Consequence 1-5	Total score 1-25	Potential drivers and enablers
O9	Different systems of competence distribution in MSs can complicate finding right authority	5	3	15	Information desk and registry of competence of authorities.
O10	Lack of trust (cultural) cross member states	4	4	16	Defining standards for data quality and procedures for validating data quality may support improved data quality as well as acceptance from other MS.
O11	Different strategies in MSs for implementation of Public services	4	4	16	Alignment of policies and deployment of frameworks like EIF with focus on cross border interoperability.
O12	Low return on investment for public services to be digitised	5	5	25	Focus on cross-sector governance and increased re-use of digital infrastructures may reduce costs for implementation and operations.
O13	Issuing and acceptance of electronically signed documents can be a challenge for authorities	4	4	16	Focus and recognition of benefits such as improved security when moving to electronic signatures as well as continued work to ease implementation of e-signatures and seals by improving generic cross-border building blocks based on eIDAS.
O14	Low uptake of eID hinders high volume demand for electronic public services, resulting in low ROI	4	4	16	Active cooperation between all levels of government to be a success. Promotion and adoption of policies supporting the process towards “Digital by Default” and “Digital Only” for public services.
O15	Lack of willingness to share data	5	5	25	Clear policies and regulation with well-defined objectives can be effective. Further documentation of results and benefits and mitigate the cultural barriers.

Table 4 Inventory of semantic risks and barriers

#	Identified risk or barrier	Probability 1-5	Consequence 1-5	Total score 1-25	Potential drivers and enablers
S1	Diverse and non-harmonized type of criteria and evidences in different member states can make it difficult to find and request relevant evidences	5	5	25	System to match criteria and evidences (Evidence Broker) and Data Services to data sources (Data Service Directory)
S2	Evidence Format and cross-MS Compatibility of Formats	5	3	15	Agreement on a common data format for structured and non-structured documents. Attached structure data whenever is possible.
S3	Missing Semantic mapping of data elements.	5	5	25	Canonical forms or common data models based on European Core Vocabularies
S4	Different levels of data quality may be a barrier on the use of data by cross-border procedures	3	3	9	The Information Desk should provide a functionality to allow the description of the data quality and data constraints of the available evidences issued by the different competent authorities. DC then can use this information to assess the usability of the evidence regarding its data quality and constraints.
S5	Identity/record matching when accessing online services cross-border	4	4	16	DC should handle the identity/record matching as required in their own country and particular situation. Possible extension of eIDAS dataset with more attributes
S6	Identity/record matching of user for data request and data access	5	5	25	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.
S7	Integration with sectoral infrastructures	5	2	10	If the procedure belongs to the same sectoral domain, the already in-place semantics can be used. Otherwise, a

#	Identified risk or barrier	Probability 1-5	Consequence 1-5	Total score 1-25	Potential drivers and enablers
					mapping between the sectorial ontology and the domain-agnostic vocabulary used for could help.
S8	Non-harmonised (or mapped) user rights, including powers and mandates	5	5	25	Development and implementation of standards and governance to cater for interoperable “Powers and Mandates” solutions cross-border – possibly extension of eIDAS to include such provisions.

Table 5 Inventory of technical risks and barriers

#	Identified risk or barrier	Probability 1-5	Consequence 1-5	Total score 1-25	Potential drivers and enablers
T1	Integration with sectoral infrastructures	5	3	15	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.
T2	Integration with national infrastructures	5	5	25	Implementation of standardised 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.
T3	The managing and governance of the choreography of distributed components managed by different agents and during a single user session.	5	5	25	Develop architectures with clear division of responsibility and simple transparent interfaces. Consistent use of standards to opening markets for commercial technology, platforms and implementations can also be a driver for improving availability of production grade solutions.
T4	Synchronicity of data exchanges	5	2	10	Investments in new technology and platforms including portal solutions for public services provisions may actually cut cost for operations and lower resources required support non digital channels and services.
T5	Current eID minimum data set only offers identity for specific point in time.	5	3	15	Extension of eIDAS eID with improved temporal management support.

5 Discussion

In the previous chapters, 38 different risks and barriers on cross-border digitised public services in every interoperability layer of the LOST model have been identified and described. Furthermore, each barrier has been assessed on the basis of its probability and consequence in order to enable a focus on the most pressing issues.

When ordering the risks and barriers according to their total score, the picture looks as follows:

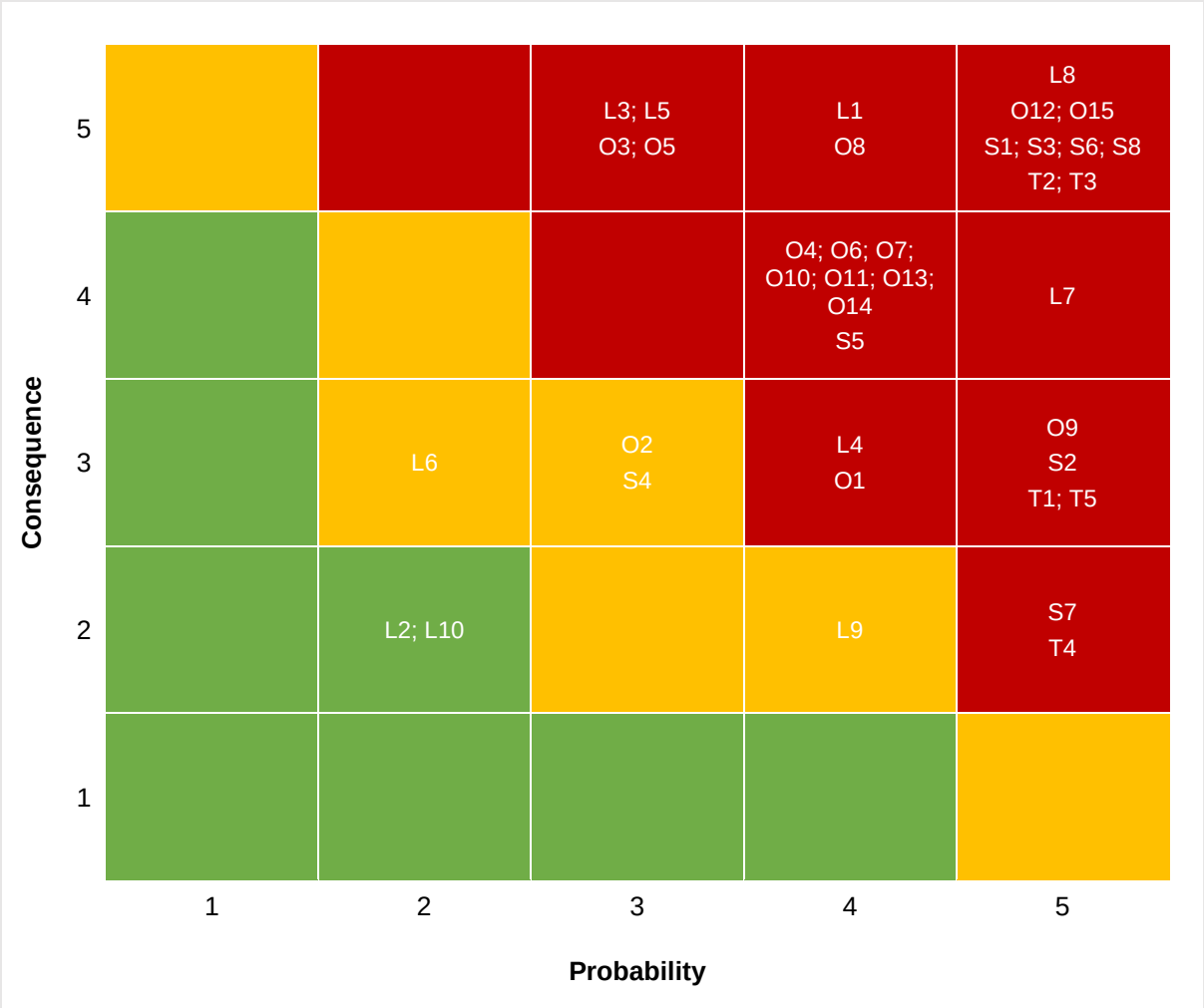

Figure 14 Overview of risks and barriers

As shown in Figure 14, most of the barriers populate the upper right-hand corner of the matrix, implying a high level of criticality. Furthermore, 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.

Even though the scores are only estimates, that the evaluation of each of the barriers has not taken into account how they may actually play out under different architectural circumstances, and that further investigation of each barrier will probably result in adjustments to several scores, the overall picture remains one of a high number of barriers with defining influence on the progress of national and European digitisation initiatives. As such, it may seem difficult to prioritise specific barriers.

However, if one may proverbially argue that where there is a will, there is a way, the high volume and criticality of organisational barriers would appear to be a good place to focus. As the general perception of implementing OOP is very favourable, that will would appear to be there. However, when considering the predominant great caution towards sharing data, low implementation levels, and reluctance to change organisational and technical structures, it could indicate that while OOP is favoured when described as an abstract concept, its realisation in terms of actual exchange of data appears to be far less appealing to the respondents. As such, there appears to be a substantial cultural barrier on cross-border services and it would appear that cross-border European services are not a core priority for many MS governments in Europe.

Different reasons could explain this: actual cross-border interaction may still be limited and converting digital infrastructure and organisational structures to meet the needs is considered too costly. Or the need for cross-border services may not be perceived urgent enough to be prioritised over other political issues when met with the harsh realities of fiscal battles.

It could also indicate that whilst the report identifies relevant drivers and enablers for the majority of risk and barriers, the actual maturation and application thereof is not a given.

The overall finding is an indication of a gap between on one side European objectives and policies and on the other the actual implementation levels and capabilities in the member states. As such, there may be reason to consider how the digital transformation in Europe required to support the Single Digital Market in the future, may best be achieved. The report's findings indicate ways of supporting that transformation.

The respondents' views on the likelihood of the various types of benefits indicate which agendas national and cross-border initiatives should cater to in order to gain support. A relatively low perception of cost savings being a benefit in cross-border implementation of OOP, suggests that successful cross-border implementation adds a complexity and requires investments that may not carry a positive ROI. Considering the low implementation levels of once only and an added complexity of cross-border implementation, the clear favouring of national implementation found in D1.3, suggest that cross-border implementation could successfully build upon national digitisation efforts.

The insights from the reports also indicate that however prone for building data and service silos, abandoning the traditional bottom-up approach of solving domain-specific and local problems is not without risk. Conversely, efforts that focus on important immediate problems will likely receive positive attention. In that regard, it is wise to take note of not only the protagonist and antagonists, but also the share of neutral parties, as it would be up to the very positive to carry the weight of the neutral, as these are otherwise likely to prioritise other matters.

Based on all of the above, this report notes that

- cross-border digitisation should build upon national digitalisation efforts;
- that digitisation initiatives should have a positive return on investment;
- initiatives that face high volume, complex and substantial barriers could benefit from a phased implementation in order to minimise implementation risks;
- effective and broadly implemented digital infrastructures supporting areas such as data-sharing, digital communication and trust-services under cross-sector governance can reduce costs and risks when implementing new services.

6 Conclusions

In this study, legal, technical, cultural and managerial risks and barriers on the implementation of cross-border digital public services have been identified.

The identification and description of the risks and barriers was based on three different kinds of sources: A survey among the Chief Information Officers of the EU and EFTA member states, a literature review of European projects, and focus group interviews with a dozen experts from 10 different countries.

By applying the framework of the LOST interoperability layers from the EIF conceptual model for integrated services, the study found and described 38 risks and barriers across the fours layers of interoperability. For each risk and barrier, drivers and enablers that may potentially mitigate the risk or overcome the barrier were presented.

The study found that when evaluating the probability and consequence of each risk and barrier, 32 of the 38 risks and barriers appear critical to address in order to be able to successfully move forward with the implementation of cross-border integrated digital public services. Furthermore, the study showed that most of risks and barriers are widespread among the EU and EFTA member states.

In each layer of interoperability, the study found that the most notable risks and barriers are

Legal

(L1) Lack of legal basis for exchanging data,

(L4) National requirements for original and /or certified copies of evidence

(L7) User Identity transitivity across borders

(L8) User consent transitivity across borders

Organisational

(O1) Lack of real-time access to data

(O6) Integrated public service governance: availability, quality and functionality

(O7) Integrated public service governance: Auditing and traceability

(O8) Different levels of data quality

(O14) Low uptake of eID hindering high volume demand resulting in low return on investment

(015) Unwillingness to share data

Semantic

(S1) Diverse and non-harmonized type of criteria and evidences

(S3) Missing Semantic mapping of data elements

(S6) Identity/record matching of user for data request and data access

(S8) Identity matching and user rights

Technical

(T1) Integration with sectoral infrastructures

(T2) Integration with national infrastructures

(T3) Governance of the choreography of distributed components

(T5) Current eID minimum data set only offers identity for specific point in time

Furthermore, the study found that although each risk or barrier may logically be categorised in either of the four layers of interoperability, each risk or barrier often has implications on the other layers, or conversely may have solutions coming from the other layers, adding further complexity to landscape of risks and barriers.

On that basis, the report discussed how the development and implementation of cross-border digital public services may best be supported. As there is a high number of critical risks and barriers in each of the four layers of interoperability, the report suggested an increased focus on organisational barriers, as overcoming these may have a positive influence on the risks and barriers of the other layers. As part of this focus on the organisational layer, the report recommended an increased focus on supporting national digitisation efforts with high return on investment.

References

[1] European Commission, "The European eGovernment Action Plan 2011-2015". 15/12/2010. Available: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0743:FIN:EN:PDF [Accessed 16/06/2020]

[2] European Commission, "EU eGovernment Action Plan 2016-2020". 19/04/2016. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0179&from=EN [Accessed 16/06/2020]

[3] European Commission, "Tallinn Declaration on eGovernment". 2017. Available: https://ec.europa.eu/digital-singlemarket/en/news/ministerial-declaration-egovernment-tallinn-declaration [Accessed 16/06/2020]

[4] European Commission, "eGovernment Benchmark 2019". 2019. Available: https://ec.europa.eu/digital-single-market/en/news/egovernment-benchmark-2019-trustgovernment-increasingly-important-people [Accessed 16/06/2020]

[5] European Commission, "The Digital Economy and Society Index (DESI)". Available: https://ec.europa.eu/digital-single-market/en/desi [Accessed 16/06/2020]

[6] European Parliament and the Council, "Regulation establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012". 02/10/2018. Available: https://eur-lex.europa.eu/eli/reg/2018/1724/oj [Accessed 16/06/2020]

[7] European Commission, "European Interoperability Framework – Implementation Strategy". 23/03/2017. Available: https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_1&format=PDF [Accessed 16/06/2020]

[8] European Parliament and the Council, "Directive (EU) 2019/1024 on open data and the re-use of public sector information". 20 June 2019. Available: https://eur-lex.europa.eu/eli/dir/2019/1024/oj [Accessed 13/07/2020]

[9] European Parliament and the Council, "Directive 2007/2/EC establishing an Infrastructure for Spatial Information in the European Community (INSPIRE)". 14 March 2007. Available: https://eur-lex.europa.eu/eli/dir/2007/2/2019-06-26 [Accessed 13/07/2020]

[10] European Parliament and the Council, "Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC". 23 July 2014. Available: https://eur-lex.europa.eu/eli/reg/2014/910/oj [Accessed 13/07/2020]

[11] European Commission, "The European Cloud Initiative". 8 November 2019. Available: https://ec.europa.eu/digital-single-market/en/%20european-cloud-initiative [Accessed 13/07/2020]

[12] European Commission, "New European Interoperability Framework". 2017. Available: https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf [Accessed 10/07/2020]

[13] Joinup, "Digital Government Factsheets". Available: https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/digital-government-factsheets [Accessed 16/06/2020]

[14] The Once-Only Project. Available: https://www.toop.eu/ [Accessed 16/06/2020]

[15] EU - SEMPER - Crossborder Semantic Interoperability of Powers and Mandates. Available: https://graz.pure.elsevier.com/en/projects/eu-semper-crossborder-semantic-interoperability-of-powers-and-man/ [Accessed 16/06/2020]

Annexes

Annex I. Calculation Methodology

The charts in this report are based on data collected from the DE4A survey (see Annex II.). The charts represent in particular the question range from 42-53 in the data strategy and Once Only section.

Chart	Indicator description	Calculation methodology
Figure 2 Average expected benefits of OOP implementation	Respondents' average opinion of national and cross-border implementation of the same beneficial outcomes of the OOP.	The responding countries answers to the likelihood of a specific beneficial outcome are transformed into a numeric scale of 1-5. Corresponding to the following answers: 1 = very unlikely 2 = unlikely 3 = neutral 4 = likely 5 = very likely The numeric average is calculated and placed on a dotted chart, corresponding to an overall average perception of the respective outcome. Not included: Answers "Other"
Figure 3 National and cross-border beneficial outcomes of OOP implementation	Respondents' opinion of national and cross-border implementation of the same beneficial outcomes of the OOP.	The chart displays the absolute number of countries replying to the likelihood of a specific beneficial outcome. An x-axis depicting percentages is added, to give an indication of the proportion of the responding countries. Not included: Answers "Other".
Figure 4 Barriers on OOP implementation	Comparison of perceived technical and non-technical barriers for OOP implementation.	The chart displays in absolute numbers the responding countries per category. An x-axis depicting percentage is added, to give an indication of the proportion of the responding countries. Not included: Answers "Other".
Figure 5 Average willingness to share data with public and private organisations	Overall indication of openness of national and cross-border data exchange to comply with OOP implementation strategies.	The responding countries answers are transformed into a numeric scale of 1-4. Corresponding to the following answers: -2 = very cautious

Chart	Indicator description	Calculation methodology
		-1 = somewhat cautious 1 = mostly open 2 = very open The numeric average is calculated and placed on a dotted chart, corresponding to an overall average perception of the respective aspect. The chart does not consider and include the answers "Unsure / no information" in the calculation. As those are neither neutral nor meaningful.
Figure 6 Willingness to share data with public and private organisations	Comparison of openness of national and cross-border data exchange to comply with OOP implementation strategies.	All given answers are separately calculated per each factor and displayed in absolute numbers. An x-axis depicting percentage is added, to give an indication of the proportion of the responding countries.
Figure 7 Willingness to share data by EU and EFTA population	Comparison of openness of national and cross-border data exchange to comply with OOP implementation strategies by EU and EFTA populations.	All given answers are separately calculated per each factor and projected onto the population of the respective responding country. The data is displayed in the percentage of the responding countries population. The underlying data does only include the population of the responding countries and thus the chart only covers 70 percent of the overall EU and EFTA population. The population data has been downloaded from Eurostat on 10/07/2020 and consists of the population on 1 January 2020.
Figure 8 Average willingness to change organisational structures and technological solutions	Overall indication of openness of national and cross-border willingness to adapt existing solutions to comply with OOP implementation strategies.	The responding countries answers are transformed into a numeric scale of 1-4. Corresponding to the following answers: -2 = very cautious -1 = somewhat cautious 1 = mostly open 2 = very open The numeric average is calculated and placed on a dotted chart, corresponding to an overall average perception of the respective aspect.

Chart	Indicator description	Calculation methodology
		The chart does not consider and include the answers "Unsure / no information" in the calculation. As those are neither neutral nor meaningful.
Figure 9 Willingness to change organisational structures and technological solutions	Comparison of openness of national / cross-border willingness to adapt existing solutions to comply with OOP implementation strategies	All given answers are separately calculated per each factor and displayed in absolute numbers. An x-axis depicting percentage is added, to give an indication of the proportion of the responding countries.
Figure 10 Specific national legislation governing OOP	Indication of specific legislation in the responding country at the national or federal level governing the OOP, i.e. 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.	For each answer category, the number of responding countries is counted and divided by the overall number of respondents. The chart depicts values in percentage to indicate the proportion of answers.
Figure 11 Procedural requirements and preconditions for data exchange	Distribution of different legal requirements for data exchange of the aforementioned national legislation.	The number of respondents per requirement is counted and divided by the overall number of respondents. An x-axis depicting absolute numbers is added, to give an indication of the number of the responding countries.
Figure 12 Legal distinction between national and cross-border data requests	Indication whether the law makes a distinction between requests coming from national public administrations compared to from other countries. For example, no transfer is allowed to foreign administrations, or a procedural requirement that in practice cannot cover foreign administrations.	The chart is based on data from a qualitative question. The answers have been quantified into the following answer possibilities: • Yes • No • Unclear • Not applicable For each answer possibility, the number of responding countries is counted and divided by the overall number of respondents.
Figure 13 Complementary sources for OOP	Distribution of supplementary legislative resources for OOP regulation, besides the aforementioned national legislation.	The number of each type of supplementary OOP regulation is counted among all countries and divided by the overall number of respondents.

Chart	Indicator description	Calculation methodology
		An x-axis depicting absolute numbers is added, to give an indication of the number of the responding countries.

Annex II. Digital Europe for All (DE4A) survey

Digital Europe for All (DE4A) survey: *Country*

Purpose of the survey and data protection

Dear member state representatives,

On January 1st of this year, the EU member state-driven project Digital Europe for All (DE4A) started. DE4A aims at 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. You can read more about the project on the project website, https://www.de4a.eu/.

The present survey that we kindly ask you to fill in, takes stock of the current deployment of cross-border services, hereby providing insights into the barriers to cross-border interoperability and the enablers to address them. The collected data will be used to analyse the current status of eGovernment in the member states in order to identify the construction base for the target technical architecture and eGovernment environment. Likewise, 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.

The survey consists of four major blocks: (1) electronic IDentification, Authentication and trust Services, (2) assessment of Life Events under Single Digital Gateway Regulations, (3) Digital Service Infrastructure, (4) Once-Only Principle and Data strategy.

We kindly ask you to express your opinion on the eGovernment advancement. The collected data will be used to create an aggregated report depicting an 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 legislative, technical, or other particularities relevant for understanding the national context. Please note that we do not request official positions of the EU member states and that no individual responses will be published.

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 the processing of your personal data. We will process your personal data 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 de-identified 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.

eIDAS: notified eID-schemes

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

.Please check the accuracy of the available information of your national eID scheme presented at the eID User Community:

National eID scheme	Level of assurance	Status	eID means
Notified_national_eID_scheme_1	LOA_1	Status_1	eID_means_1
Notified_national_eID_scheme_2	LOA_2	Status_2	eID_means_2
Notified_national_eID_scheme_3	LOA_3	Status_3	eID_means_3

If there are any updates with regards to the (pre-)notified eID scheme(s) (e.g., level of assurance, current notification status), please leave a comment in the following text box.

……

.The eID scheme is operated by:

	Public entity	Private entity	Public-private partnership	Do not know / Other (please specify)
Notified_national_eID_scheme_1				
Notified_national_eID_scheme_2				
Notified_national_eID_scheme_3				

Other (please specify) ……

.The implementation level of eID scheme is:

	Not implemented	Necessary legislation adopted	Implemented for national use	Implemented for cross-border use	Do not know / Other (please specify)
Notified_national_eID_scheme_1					
Notified_national_eID_scheme_2					
Notified_national_eID_scheme_3					

Other (please specify) ……

.The eID scheme grants access to:

	National public services	Public services from regional / local authorities	Non-governmental services (e.g. Banking, Telecom) - please specify	Do not know

Notified_national_eID_scheme_1				
Notified_national_eID_scheme_2				
Notified_national_eID_scheme_3				

Other (please specify) ……

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

Notified_national_eID_scheme_1 ……

Notified_national_eID_scheme_2 ……

Notified_national_eID_scheme_3 ……

.Please indicate activation rate for all the listed eID schemes where applicable. *Activation rate is a cumulative ratio of activated eIDs to total number of eIDs.*

Notified_national_eID_scheme_1 ……

Notified_national_eID_scheme_2 ……

Notified_national_eID_scheme_3 ……

.Please indicate use rate for all the listed eID schemes where applicable. *Use rate is a cumulative ratio of eIDs which have been used at least once to access a public service to the total number of eIDs.*

Notified_national_eID_scheme_1 ……

Notified_national_eID_scheme_2 ……

Notified_national_eID_scheme_3 ……

.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.

……

.Are there any other national eID schemes in operation which have not been listed in this subchapter?

eIDAS: new eID schemes

This subchapter only appears, if in question 9 answer "yes" is selected

Please provide information concerning operating national eID schemes.

.Please insert below the name(s) of your new national eID scheme(s):

eID_scheme_1 ……

eID_scheme_2 ……

eID_scheme_3 ……

eID_scheme_4 ……

eID_scheme_5 ……

11.Please indicate the corresponding level of assurance of the eID scheme(s):

	Low	Low	High	Not relevant / Do not know

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

Other (please specify) ……

*** 12. Please identify the level implementation of the eID scheme(s):**

	Necessary legislation adopted	Implemented for national use	Implemented for cross-border use	Not relevant / do not know
eID scheme (1)				
eID scheme (2)				
eID scheme (3)				
eID scheme (4)				
eID scheme (5)				

Other (please specify) ……

.The eID scheme(s) is/are operated by:

	Public entity	Private entity	Public-private partnership	Not relevant / Do not know
eID scheme (1)				
eID scheme (2)				
eID scheme (3)				
eID scheme (4)				
eID scheme (5)				

Other (please specify) ……

.The eID scheme(s) grant(s) access to:

	National public services	Public services by regional / local authorities	Non-governmental services (e.g. Banking, Telecom) - please specify	Not relevant / Do not know
eID scheme (1)				
eID scheme (2)				
eID scheme (3)				
eID scheme (4)				
eID scheme (5)				

Other (please specify) ……

15. Please indicate possession rate for all the listed eID schemes. *Possessions rate is a ratio of total number of eID holders to total number of inhabitants (citizens + foreign residents).*

eID_scheme_1 ……

eID_scheme_2 ……

eID_scheme_3 ……

eID_scheme_4 ……

eID_scheme_5 ……

.Please indicate activation rate for all the listed eID schemes where applicable. *Activation rate is a cumulative ratio of activated eIDs to total number of eIDs.*

eID_scheme_1 ……

eID_scheme_2 ……

eID_scheme_3 ……

eID_scheme_4 ……

eID_scheme_5 ……

.Please indicate use rate for all the listed eID schemes where applicable. *Use rate is a cumulative ratio of eIDs which have been used at least once to access a public service to the total number of eIDs.*

eID_scheme_1 ……

eID_scheme_2 ……

eID_scheme_3 ……

eID_scheme_4 ……

eID_scheme_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.

……

eIDAS: eIDAS-Node and trust services

.Does your eIDAS-node support using your national eID's abroad?

……

.Does your eIDAS-node support foreign eIDS's to be used for services in your country?

……

.The Regulation on electronic identification and trust services (eIDAS) foresees the implementation of eSignature, eSeal and Timestamps. Please identify the advancement level of those services in your country:

	Do not know	Not implemented	Necessary legislative procedures adopted	Implemented for national use	Implemented for cross-border use
Electronic Signature					

Advanced Electronic Signature					
Qualified Electronic Signature					
Electronic Seal					
Advanced Electronic Seal					
Qualified Electronic Seal					
Electronic TimeStamp					
Qualified Electronic TimeStamp					

.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.

……

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.

.Please indicate the level of online availability of information, service and assistance with respect to the mentioned procedures:

Online authentication, possible answers from drop-down list: (1) Personal presence, (2) Online, non-eID, (3) Online, eID-enabled, (4) Do not know, (5) Not applicable

Implementation of the OOP (data reuse), possible answers from drop-down list: (1) No, (2) Planned, not technically implemented, (3) Yes, reuse of unstructured data, (4) Yes, reuse of structured data, (5) Do not know, (6) Not applicable

Mobile accessibility, possible answers from drop-down list: (1) No, (2) Only desktop enabled website, (3) Mobile-enabled website, (4) Dedicated eGov app, (5) Do not know, (6) Not applicable

Online availability for cross-border use, possible answers from drop-down list: (1) No, (2) Yes, information available online, (3) Yes, information and services available online, (5) Do not know, (6) Not applicable

	Online authentication	**Implementation of the OOP (data reuse)**	**Mobile accessibility**	**Online availability for cross-border use**
Requesting proof of registration of birth				
Requesting proof of residence				
Applying for a tertiary education study financing				
Submitting an initial application for admission to public tertiary education institution				

Requesting academic recognition of diplomas, certificates or other proof of studies or courses				
Request for determination of applicable legislation in accordance with Title II of Regulation (EC) No 883/2004 (1)				
Notifying changes in the personal or professional circumstances of the person receiving social security benefits				
Application for a European Health Insurance Card				
Submitting an income tax declaration				
Registering a change of address				
Registering a motor vehicle originating from or already registered in a Member State				
Obtaining stickers for the use of the national road infrastructure				
Obtaining emission stickers issued by a public body or institution				
Claiming pension and pre-retirement benefits from compulsory schemes				
Requesting information on the data related to pension from compulsory schemes				
Business activity: Notification, permission for exercising, changes and termination				
Registration of an employer with compulsory pension and insurance schemes				
Registration of employees with compulsory pension and insurance schemes				

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

.Are there any procedural frameworks in place, which reckon for involvement of other parties (e.g., private entities, end-users etc.) in the process of co-creation?

……

.What is approximate percentage of services available digitally as compared to overall number of public, administrative services

at national level……

at regional/local level……

.What is approximate percentage of digital-only services (*services available exclusively online*)?

at national level……

at regional/local level……

.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.

……

Digital Service Infrastructure

The aim of this subchapter is to identify the level of 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.

.Please indicate the level of advancement of the DSIs listed below:

	Do not know	Not implemented	Necessary legislative procedures adopted	Fully/partially Implemented for national use
EU Student eCard				
eDelivery				
eInvoicing				
Access to re-usable public sector information – Public Open Data				
Automated Translation				
Critical digital infrastructures support – Cybersecurity				
eProcurement				
eHealth - ePrescriptions				

eHealth - cross-border patient data sharing				
Business registers interconnection system				
Electronic exchange of social security information				
e-Justice - Use case of citizens				
e-Justice - Use case of businesses				
Online Dispute Resolution				

.Please indicate implemented and running use cases of Blockchain technology for the purpose of provision of public services (name and a brief description of its implication - e.g. public procurement, internal financial audit etc.):

……

.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 measures the member states' implementation of the Once-Only Principle (OOP) and reuse of data principle. Enshrined in the eGovernment Action Plan, the OOP implies the 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.

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

Do not know

No

Yes (please provide a link) ……

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

A national strategy of reusing public sector data in the public sector

A national strategy for harmonization of data across select registries

A national strategy for Open Data

Implementation of Open Data by default

One or more national catalogs of data sets to make data findable

A national governance implementation supporting data access

Other (please specify) ……

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

Persons/citizens

Vehicle

Tax

Businesses

Addresses

Building and housing

Cadasters

Geographical data

Higher Education

None

Other (please specify) …….

34. Please elaborate on the types of private companies which can access base registries and the access conditions:

…….

35. Please indicate how the access to base registries is implemented. Check all that apply.

Replication of registries to authorities that need access

Data lookup supported by API's

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) …….

36. Are there any fees introduced for access to cross-border registries for private and public organizations?

Possible answers of drop-down lists: (1) Yes, (2) No, (3) Do not know

	Public organizations	Private organizations
Are there fees applied for national transactions?		
Are there fees applied for cross-border transactions?		
Are there fees intended to be applied for cross-border transactions?		

Other (please specify) …….

37. 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

38. Please check 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 verify access to their data by others	Not applicable in my country	Do not know
Personal file					
Tax declarations					
Medical file					

Cadasters (private property)					
Personal mandates					
None					

Other (please specify) ……

39. To what extend is OOP implemented in your country? Check all that apply.

OOP is implemented broadly at the national level

OOP is implemented in certain areas or organisations at the national level

OOP is implemented broadly at the regional level

OOP is implemented in certain areas/organisations at the regional level

OOP is implemented at all levels of power

Do not know

Other (please specify) ……

40. In what cross-border OOP initiatives is/has your country been involved? Check all that apply.

The Once-Only-Principle (TOOP)

Business Registers Interconnection System (BRIS)

Stakeholder Community Once-Only Principle for Citizens (SCOOP4C)

European Criminal Records Information System (ECRIS)

European Data Interchange for Waste Notification Systems (EUDIN)

Connecting European Facility (CEF) programs

Simple Procedures Online for Cross-Border Services (SPOCS)

Interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA2)

None

Other (please specify) ……

41. In your opinion, what would be beneficial outcomes of national implementation of the OOP? Please specify in the textbox below any further expected benefits for your government from the national OOP implementation:

	Very unlikely	Unlikely	Neutral	Likely	Very likely
Efficiency					
Administrative simplification					
Time savings					
Cost savings					
Increased collaboration between agencies					
Better governance					
Avoidance of duplication of tasks					

Increased data quality and reliability					
Increased interoperability					
Increased transparency and accountability					
Fraud reduction					

Other (please specify) ……

42. In your opinion, what would be beneficial outcomes of cross-border implementation of the OOP? Please specify in the textbox below any further expected benefits for your government from the cross-border OOP implementation:

	Very unlikely	Unlikely	Neutral	Likely	Very likely
Efficiency					
Administrative simplification					
Time savings					
Cost savings					
Increased collaboration between agencies					
Better governance					
Avoidance of duplication of tasks					
Increased data quality and reliability					
Increased interoperability					
Increased transparency and accountability					
Fraud reduction					

Other (please specify) ……

43. How would you evaluate the likelihood of the following national, administrative factors to impede the European OOP implementation for your government?

	Not a barrier	Moderate barrier	Substantial barrier	Extreme barrier
Absence / insufficiency of national legislative framework				
Incompatibility of national legislative frameworks of the EU member states				
Administrative complexity / Organizational silos				
Organizational resistance to changes				
Organizational and cultural differences among stakeholders				
Lack of financial resources				
Asymmetric costs distribution in the cross-border context				

Costs of sustaining the services in the long-term				
Lack of relevant human resources				
Political vulnerability and lack of political support				
Low take-up, low expectancy of number of potential users				
Different OOP levels in other EU member states				

Other (please specify) ……

44. How would you evaluate the likelihood of the following technical factors to impede the OOP implementation for your government?

	Not a barrier	Moderate barrier	Substantial barrier	Extreme barrier
Incompatibility of IT-processes / IT-standards / used technologies				
Data incompatibility				
Deficient data quality				
Semantic incompatibility of information systems and used datasets				
Uneven quality of used technologies to ensure quality and security of the transferred and used data				

Other (please specify) ……

45. Is there specific legislation in your country at the national or federal level governing the OOP, i.e. 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?

No

Do not know

Yes (please provide a link to the relevant law) ……

46. What sources of data are covered (i.e. what databases or data sources fall under the once-only principle and can be exchanged under the principle) by the respective legislation?

……

47. What are the procedural requirements or preconditions for an exchange under the respective legislation? Check all that apply.

No conditions – any party may receive and use our data as-is without restrictions or prior authentication (data is shared as open data)

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 receiving administrations

Obligation to use certain data formats

Obligation to use 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

Other (please specify) ……

48. Does the law make a distinction between requests coming from public administrations in your own country compared to from other countries? Specifically, is there any part of the law that makes it impossible or harder for your administrations to apply the OOP towards requesting administrations in or from other countries than your own (e.g. no transfer is allowed to foreign administrations, or there is a procedural requirement that in practice cannot cover foreign administrations)? If so, please describe the relevant provisions.

……

59. What are other sources of OOP regulation 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) ……

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

	Unsure / no information	Very cautious	Somewhat cautious	Mostly open	Very open
Sharing data with public organizations within the country					
Sharing data with private organizations within the country					
Sharing data with other countries					
Sharing personal data with public organizations in the country					
Sharing personal data with private organizations in the country					
Sharing personal data with other countries					
Changing existing organizational processes, procedures and structures to enable OOP nationally					
Changing existing organizational processes, procedures and structures to enable cross-border OOP					
Changing existing technological solutions (information systems, architectures), etc. to enable OOP nationally					
Changing existing technological solutions (information systems, architectures), etc. to enable cross-border OOP					

51. 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:

……