The Once-Only Principle Project

Overview of legal landscape and regulations

Hans Graux

Submitted to the EC on 29/08/2017

Horizon 2020 – The EU Framework Programme for Research and Innovation

PROJECT ACRONYM: TOOP

PROJECT FULL TITLE: The "Once-Only" Principle Project

H2020 Call: H2020-SC6-CO-CREATION-2016-2

H2020 Topic: CO-CREATION-05-2016 - Co-creation between public administrations: once-only principle

GRANT AGREEMENT n°: 737460

D2.5. Overview of legal landscape and regulations

Deliverable Id :	D2.5
Deliverable Name :	Overview of legal landscape and regulations
Version :	V1.0
Status :	Final
Dissemination Level :	Public
Due date of deliverable :	M8 (August 2017)
Actual submission date :	29/08/2017
Work Package :	WP2
Organisation name of lead partner for this deliverable:	e-SENS.com
Author(s):	Hans Graux
Partner(s) contributing:	Time.lex, Bundesrechenzentrum Gmbh, Brønnøysundregistrene

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Abstract:
This deliverable includes an inventory of the legal landscape and the regulations (both existing and emerging) that will have an impact on TOOP pilot activities across the Pilot Areas. It focuses on the legal drivers and barriers and explains how these barriers will be addressed within the context of TOOP.
The overall structure and logic of the deliverable emerges from the need to ensure that TOOP:

- Complies with existing legislation and satisfies national legal and policy requirements;
- Provides a framework that can be applied to other pilots outside the context of TOOP (i.e. to ensure that the solution approach can be generalised to other once-only use cases);
- Is in line with emerging legislation on the once-only principle, including specifically the recently proposed Single Digital Gateway Regulation.

In order to meet these objectives, this deliverable firstly identifies key legal principles with a basis in EU law, in order to identify horizontally applicable rules that govern the application of the once-only principle, and to create a legal assessment framework that allows legal barriers and challenges to be identified in any once-only use case.

Secondly, it identifies and describes specific applicable legislation per pilot area in order to identify concrete legal requirements for the execution of the pilots. In practical terms, this can be understood as the application of the legal assessment framework to the three selected pilot areas.

Thirdly, it proposes a legal solution framework (i.e. a set of legal tools) that can be applied in the three pilot areas to ensure that TOOP operates in compliance with existing law.

The next steps, which are not yet fully developed in the present report, although an initial outline is provided, will be to instantiate the toolbox, i.e. to draft specific framework agreements, terms and conditions and policies that can be used in the actual development and roll-out of the pilots, which will be created in cooperation with pilot leaders. These texts are not incorporated in this deliverable, since the motivational scenarios of the pilots are still under development, but will be reported on as a part of D2.13 (sustainability plan).

In addition, in the course of the TOOP project the legal drivers and barriers are reiterated and re-evaluated within D2.13 (sustainability plan), based on the experiences in the pilots, in order to ensure the long-term usability of TOOP outputs, taking into account the development of the Single Digital Gateway Regulation in the course of the project.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Table of contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

List of Figures

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

List of Tables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

List of Abbreviations

Acronym	Explanation
ABB	Architecture Building Block
BB	Building Block
BRIS	Business Registers Interconnection System
CEF	Connecting Europe Facility
DPD	Data Protection Directive 95/46/EC
DSI	Digital Service Infrastructure
eIDAS	electronic Identification and Signature
EIF	European Interoperability Framework
EIRA	European Interoperability Reference Architecture
EO	Economic Operator
EES	ETSI Rationalised Framework for Enhanced Security Services
GDPR	General Data Protection Regulation (EU) 2016/679
LSP	Large Scale Pilot
MA	Maritime Administration
OOP	„Once-Only“ Principle
PA	Pilot Area
PKI	Public Key Infrastructure
PSC	Port State Control
SAT	Solution Architecture Template
SDGR	Single Digital Gateway Regulation
SML	Service Metadata Locator
SBB	Solution Building Block
TOOP	The “Once-Only” Principle Project
WP	Work Package

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

Executive Summary

The “Once-Only” Principle Project (TOOP) is about exploring, demonstrating, and enabling the “once-only” principle in the European Union. This is done by implementing three “once-only” pilot projects (TOOP pilots), by developing a generic federated OOP architecture, and by exploring other aspects of OOP and its supporting infrastructure such as OOP drivers and barriers.

Within TOOP, Task 2.2 (Legal Landscape) focuses on the identification of legal drivers and barriers for the implementation and application of the once-only principle, both horizontally (i.e. without considering the specificities of specific pilots or use cases) and by looking at the three selected pilot projects. This task therefore provides an analytical framework that allows legal challenges for once-only initiatives to be identified, which is thereafter applied to the pilot usage scenarios, in order to identify and address their specific legal challenges.

More in detail, T2.2. requires:

- The identification and evaluation of general principles with a basis in EU law, e.g. subsidiarity, data protection, data sovereignty, purpose limitation, liability, and their impact on the application of the once-only principle at the cross-border level;
- Identification and evaluation of relevant European legislation, e.g. eIDAS, the General Data Protection Regulation (GDPR), the PSI-II-Directive, and their impact on the application of OOP at the cross-border level;
- Identification and evaluation of relevant national legislation in Member States and Associated Countries that are participating in the pilots of WP3, and for any additional Member States and Associated Countries where such information is publicly available (e.g. on the basis of prior initiatives or studies).

In order to meet these objectives, this deliverable firstly identifies key legal principles with a basis in EU law, in order to identify applicable generic legal principles that will govern any use cases of the once-only principle; and to create a legal assessment framework that allows legal barriers and challenges to be identified in any once-only use case (Chapter 2 of this deliverable). Methodologically, this was done by evaluating relevant EU level legal texts at the general level – i.e. without going into the legislation governing individual use cases or specific pilot contexts – and attempting to extract or derive general principles that will need to be adhered to when applying the once-only principle.

Key source documents were the EU Charter of Fundamental Rights, the General Data Protection Regulation, the recently proposed Single Digital Gateway Regulation, the eIDAS Regulation, the PSI-II Directive, the Services Directive and the e-Commerce Directive. While not comprehensive, this regulatory package was selected in order to extract legislation that was most likely to impact once-only use cases, driven by TOOP Deliverables: TOOP D2.7 - Drivers and barriers for OOP (2017), TOOP D2.6 - Position Paper on Definition of the “Once-Only” Principle (2017); and TOOP D2.1 Generic Federated OOP Architecture (1st version) (2017). These describe the context of the once-only principle in general, and its impact on the TOOP pilots in particular. The present deliverable adds to this analysis by linking this analysis to legislation and legal principles.

This is not a theoretical or academic exercise: the legal assessment framework created in Chapter 2 is used in practice to execute domain-specific analyses for specific piloting use cases. This deliverable demonstrates how this principle can be applied in Chapter 3, where the legal assessment framework is applied to each of the three pilot areas. In practice, this requires two steps:

- For each pilot area, we firstly identify and describe specific applicable legislation in order to identify concrete legal requirements for the execution of the pilots. This is necessary since the legal assessment framework defined in Chapter 2 is generic and application-neutral: it does

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

not consider the specificities that might be introduced by specific laws or policies. Therefore, the first step of each pilot area assessment is the completion of the legal assessment framework by identifying relevant laws and policies, and extracting any relevant legal requirements.

- Once the first step is completed, the legal assessment framework as drafted in Chapter 2 is applied as well, in order to identify where potential challenges might occur.

The outcome is a statement of legal requirements that must be satisfied in order to implement a specific pilot area.

Of course, the objective of task 2.2 is not only to identify legal requirements, but also to identify potential solutions. Since the Single Digital Gateway Regulation was only proposed on 2 May 2017 and is presently still in the proposal stage, a legal toolset is defined in Chapter 4 that can be applied in the three pilot areas to ensure that TOOP operates in compliance with existing law. This includes a description of framework agreements, terms and conditions, privacy policies and so forth, which can be instantiated (i.e. drafted and applied in a pilot-specific form) during the TOOP project in order to ensure that the pilots can be executed in practice in accordance with applicable legal requirements.

The next steps, which are not yet fully developed in the present report, although an initial outline is provided, will be to instantiate the toolbox, i.e. to draft specific framework agreements, terms and conditions and policies that can be used in the actual development and roll-out of the pilots, which will be created in cooperation with pilot leaders. These texts are not incorporated in this deliverable, since the motivational scenarios of the pilots are still under development, but will be reported on as a part of TOOP D2.13 (sustainability plan).

In addition, in the course of the TOOP project the legal drivers and barriers are reiterated and re-evaluated as part of TOOP D2.13 (sustainability plan), based on the experiences in the pilots, in order to ensure the long-term usability of TOOP outputs, taking into account the development of the Single Digital Gateway Regulation in the course of the project.

The main conclusions of this deliverable are that:

- The three pilot areas can be executed in compliance with current legislation. However, in the current absence of a generic legal framework for supporting the once-only principle (with the SDGR not yet having entered into force), the pilots need to be legally supported by an appropriate contractual framework. This can be done within the context of T2.2, but is of course resource intensive (since contracts must be created on a case by case basis, and every participant must sign the agreement individually), somewhat unpredictable (since it depends on a willingness to sign), and prone to discussion (since any participant may ask that contracts are opened for negotiation). Furthermore, there is one variable which a pilot project such as TOOP cannot control: if a participant feels that it would be contrary to its legal mandate to participate in the TOOP project (e.g. a public administration refuses to make its data available to its counterparts in other Member States because it has no explicit legal mandate to do so), there is no legal recourse to require it to participate. As will be explained below, the risk is manageable within TOOP as all three pilots have a legal basis for at least part of their functionality, even in the absence of a general legal framework such as the SDGR.
- Further assessment is needed as to how the contractual setup of TOOP can be integrated into the long-term vision of the SDGR. It is clear that the TOOP infrastructure could evolve into the 'technical infrastructure' envisaged by Article 12 of the SDGR as will be explained in the sections below, and therefore that some of the solutions envisaged by this deliverable could plausibly be integrated into the implementing acts contemplated by Article 12, thus ensuring that the lessons learned in TOOP can be adopted in the implementation of the SDGR. However,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

this will require some further maturing, both of the SDGR (the proposal as such is still relatively recent and may therefore still be refined) and of the solutions proposed in this report (as the pilots must still be implemented).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

1. Introduction

Scope and Objective of this Deliverable

The objective of the current TOOP Deliverable D2.5 is to identify legal drivers and barriers for the implementation and application of the once-only principle, in order to provide an analytical framework for the pilot usage scenarios to identify and address their specific legal challenges.

More in detail, T2.2. requires:

- The identification and evaluation of general principles with a basis in EU law, e.g. subsidiarity, data protection, data sovereignty, purpose limitation, liability, and their impact on the application of the once-only principle at the cross-border level;
- Identification and evaluation of relevant European legislation, e.g. eIDAS, the General Data Protection Regulation (GDPR), the PSI-II-Directive, and their impact on the application of OOP at the cross-border level;
- Identification and evaluation of relevant national legislation in Member States and Associated Countries that are participating in the pilots of WP3, and for any additional Member States and Associated Countries where such information is publicly available (e.g. on the basis of prior initiatives or studies);

Specifically, the Deliverable achieves these goals by:

- Defining a generic legal assessment framework, on the basis of EU level legislation, that can be used to identify legal challenges and requirements for any once-only use case (chapter 2 of the Deliverable).
- Conducting a legal assessment of the three pilot areas, specifically by identifying any pilot-specific legislation, policies and legal requirements, and combining these with the application of the legal assessment framework to arrive to a concise statement of legal challenges which are specific to the pilot area (chapter 3 of the Deliverable).
- Defining the legal toolbox that will be used to create a legal framework for once-only use cases (chapter 4 of the Deliverable).
- Providing a high-level initial definition of legal solution models for the three pilot areas (chapter 5 of the Deliverable).

The high-level definition of legal solution models will be developed and made more concrete in the course of the TOOP project, and further refinement of the work in this Deliverable will be incorporated in TOOP D2.13 (sustainability plan), based on the experiences in the pilots, in order to ensure the long-term usability of TOOP outputs, taking into account the development of the Single Digital Gateway Regulation in the course of the project.

WP2 General Objectives and Vision

The general objectives of TOOP WP2 (Technical Architecture, Legal and Governance Aspects) are to develop a generic, federated OOP architecture, to create a framework for development of specific architectures and applications for TOOP, to develop a profile specification of the common building blocks, to identify general legal barriers and drivers regarding privacy, confidentiality and consent needed for the implementation of OOP, to assess the possible impacts of the implementation of OOP in the pilots in WP3, as well as to define a sustainability plan for the maintenance of the architectures, building blocks and drivers/barriers after the end of the project.

The results of WP2 represent the main technological innovation of TOOP - the generic federated OOP architecture that supports the interconnection and interoperability of national registries at the EU level - together with other investigations needed to generalize, extend, and sustain the TOOP results.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Relations to Internal TOOP Environment

The current deliverable presents legal requirements in relation to the OOP, both at the generic level and for each PA, and provides a solution for complying with these legal requirements. On the basis of this Deliverable, legal tools will be offered to pilot participants, tailored to each PA and to the requirements of the participants, in order to ensure that the piloting can occur in compliance with applicable law.

The deliverable will share its outcomes with other WP2 tasks, and provides legal support to WP3 within the scope of task T2.5. Specific instantiations of the legal tools will be implemented as a part of T2.2 throughout the continuation of the project during the development of the TOOP pilot projects in WP3. The legal analysis is partially based on the interaction between WP2 and WP3, on the questionnaire[1] and information provided with respect to other tasks in WP2, and other sources. Maintaining and further development of the architecture will be planned by the Sustainability and Governance task of WP2.

Relations to External TOOP Environment

As indicated above, external pre-existing legal inputs are the basis for the creation of the legal assessment framework (Chapter 2) and for the legal assessment of the three pilot areas (Chapter 3). Furthermore, this Deliverable also aims to support the further development of the proposed SDGR, potentially including its implementing acts after its adoption, by establishing the challenges encountered and solutions pilots from a legal perspective within TOOP.

Legal Issues

The identification and resolution of legal issues related to European legislation, as well as to national legislation in Member States and Associated Countries that are participating in the pilots of WP3, is the core focus of the present Deliverable. The solutions found can be executed in compliance with current legislation through an appropriate contractual framework, as will be explained below. In the longer term, operating on a regulatory basis (such as the recently proposed SDGR) would resolve some of the challenges which are expected to emerge as a result of the reliance on a contractual framework within TOOP, but this will likely not take place for some time after the conclusion of TOOP.

Structure of the Document

The Deliverable includes five chapters. This first chapter, the Introduction, gives an overview and background of the deliverable.

The second chapter defines the legal assessment framework, i.e. the general principles with a basis in EU law that should be adhered to in all once-only use cases.

In the third chapter, a legal assessment of the three pilot areas is done, firstly by identifying any specific legal and policy requirements that are unique to the PAs, and secondly by applying the legal assessment framework to the PAs. The outcome is a concise statement of legal challenges which are specific to each pilot area.

Chapter four defines the legal toolbox that will be used to create a contractual legal framework for once-only use cases within the context of TOOP at an abstract level, and chapter 5 finally provides a high-level initial definition of legal solution models for each of the three pilot areas.

[1] Available as Appendix I in TOOP Deliverable D2.7 (2017)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

2. Defining the legal assessment framework

Introduction

This section aims to define a generic legal assessment framework that allows legal challenges for any once-only initiatives to be identified. The outcome should consist of a statement of principles that can be used as assessment criteria to determine whether any once-only scenario is likely to encounter specific types of legal challenges and what the resulting requirements might be. The logical structure therefore looks as follows:

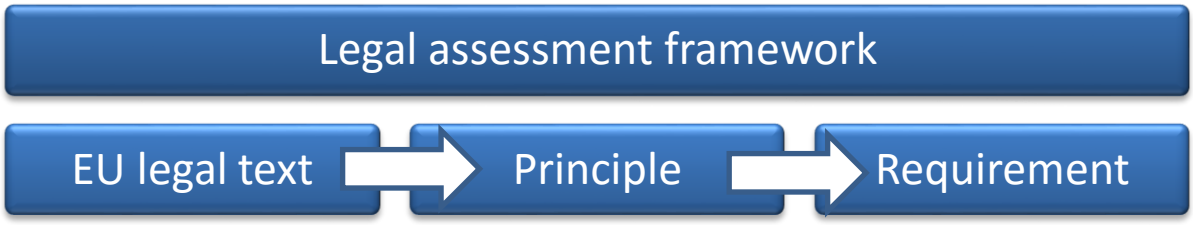

Figure 1: Legal assessment framework: an EU legal text is the source of a principle, which defines requirements

Given this scoping, the following principles apply to the legal assessment framework:

- The legal assessment framework, including the principles and the resulting requirements, must be **generic**, in the sense that it must be possible to apply the framework to any once-only use case. No sector or context specific principles or requirements will be defined.
- The legal assessment framework must be defined at the **European** level. This means that only EU level sources are used to define principles and requirements, excluding international, national or regional sources.
- The legal assessment framework must be **based in law**, in the sense that only legal texts are used as sources for principles and thus requirements. This excludes policy statements or preferences, and ethical requirements.
- The legal assessment framework must result in **requirements**: it is not a collection of legal source material and abstract principles, but must contain specific requirements that can be applied to once-only use cases.
- The legal assessment framework must be **testable**, meaning that it must be possible to apply each of the requirements to a once-only use case and to determine whether it has been complied with.

Methodologically, the legal assessment framework will be created by evaluating relevant EU level legal texts that meet the requirements of being generic – i.e. without going into the legislation governing individual use cases or specific pilot contexts – and attempting to extract or derive general principles that will need to be adhered to when applying the once-only principle. Multiple texts can obviously support the same principles and even result in the same requirements; i.e. while each requirement and principle can be traced to at least one legal source, some requirements and principles are supported by multiple legal sources.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Sources, selection logic and relevance to the OOP

As noted above, the legal assessment framework is based on EU level legal texts as a source. This implies that a first selection had to be made of texts that were considered as relevant. The selection process was conducted based on three factors:

- Firstly, a review of policy documents and studies[2] was conducted to determine which legal sources were identified as relevant in determining the requirements for compliance with the once-only principle.
- Secondly, inputs from discussions with PA leaders were taken into account, since they are most likely to be intimately familiar with key legal requirements. The outcomes were formalised notably in TOOP D2.7 (2017), and TOOP D2.6 (2017). These describe the context of the once-only principle in general, and its impact on the TOOP pilots in particular. The present deliverable adds to this analysis by linking this analysis to legislation and legal principles.
- Thirdly, relevant national level legislation was identified and evaluated in order to derive key legal principles; an overview of this legislation can be found in Annex I to this Deliverable.

The outcome of this process was the following list of source documents were used, with the justifications indicated below.

Source	Justification for its selection
EU Charter of Fundamental Rights	While generic, the Charter states the fundamental rights that should be observed by the institutions and bodies of the EU, and by national authorities only when they are implementing EU law. It includes testable rights that are critical to the correct application of the OOP, such as the right to good administration (including transparency and impartiality), the right to justice (right to appeal and the right to be heard), and the right to privacy / data protection.
Data Protection Directive (DPD) and General Data Protection Regulation (GDPR)	The right to data protection is a fundamental right as indicated in the Charter, and implies that any OOP use case where personal data is processed will need to adhere to applicable data protection law. Until 25 May 2018, the DPD (or rather its national transpositions) apply; thereafter the national data protection laws will largely be supplanted by the GDPR.
Proposal for a Single Digital Gateway Regulation (SDGR)	The SDGR aims to create a legal basis for the OOP[3]. Article 12 provides for a mechanism for the electronic exchange of evidence upon explicit

[2] Notably the 2012 Study on eGovernment and the Reduction of Administrative Burden, the 2016 EU eGovernment Action Plan 2016-2020 - Accelerating the digital transformation of government, and the 2017 study on the EU-wide digital Once-Only Principle for citizens and businesses - Policy options and their impacts

[3] It is worth noting that a separate legal initiative exists which may create a separate legal basis for the once-only principle towards the European Commission, via the Proposal for a Regulation setting out the conditions and procedure by which the Commission may request undertakings and associations of undertakings to provide information in relation to the internal market and related areas. Specifically, Article 5 of the proposal notes that "*The Commission shall only use the power to request information from undertakings and associations of undertakings provided for in Article 4 where the information available to the Commission, required for the purpose referred to in Article 4, is not sufficient or adequate and cannot be obtained in a timely manner due to the following reasons:*

(a) the information is not contained in a publicly available source; and

(b) the information has not been provided by a Member State upon request by the Commission; or

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

	request by the user. This aims to directly support the use of the "once-only" principle for the purpose of the exchange of evidence between competent authorities in different Member States. The SDGR even contains a description of the OOP, stating that it "means that citizens and businesses should not have to supply the same information to public authorities more than once for the cross-border exchange of evidence". While still a proposal and therefore still subject to changes, it can thus be critically important for supporting the OOP from a legal perspective.
eIDAS Regulation	The eIDAS Regulation provides a homogeneous legal framework for electronic identification and certain trust services (including electronic signatures) across the EU. The identification of citizens and businesses will be critical to the successful implementation of the OOP: if, as the SDGR states, the objective is to ensure that evidence on citizens and businesses can be exchanged directly between competent authorities, it must be possible for the competent authorities to uniquely identify[4] the citizens and businesses with adequate certainty in order to determine which evidence pertains to them.
PSI-II Directive	The Public Sector Information Directives (the PSI and PSI II Directive) contain an important principle: not all information controlled by public administrations is subject to rigid access and re-use requirements. While the OOP will not necessarily relate to information that would be available as open data under the PSI Directives, it is none the less important not to assume that advanced legal controls are a legal prerequisite in all cases.
Services Directive	The Services Directive aims to support the free movement of services in the internal market by removing legal and administrative barriers to trade for the services within its scope. While it does not govern the OOP as such, it contains administrative simplification obligations and implementation measures (such as the creation of national Points of Single Contact) that aim to ensure that service providers can easily exchange trustworthy electronic information from one Member State to the next in order to be permitted to offer their services in another Member State than where they are established. The Services Directive does not comprise any OOP implementation, although it is supported by the Internal Market System (IMI) that facilitates the validation of such exchanged information.
e-Commerce Directive	While not applicable to interactions between competent authorities as the OOP would require, the e-Commerce Directive none the less is indirectly relevant for its statement of key legal principles in online interactions, including with respect to the validity of electronic transactions, information and transparency requirements, liability and dispute settlement in cross border contexts.

Table 1: Legal source documents for the legal assessment framework

(c) the information has not been provided by a legal or a natural person". See http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0257&from=EN

[4] Under the eIDAS Regulation Article 2 (1), electronic identification "means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person"; thus, electronic identification under eIDAS should permit the unique identification of natural persons and businesses.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

While not comprehensive, this regulatory package was selected in order to extract legislation that was most likely to impact once-only use cases and that would be useful in order to identify relevant legal principles. While not comprehensive, this regulatory package was selected in order to extract legislation that was most likely to impact once-only use cases, driven by TOOP D2.7 (2017), TOOP D2.6 (2017); and TOOP D2.1 (2017). These describe the context of the once-only principle in general, and its impact on the TOOP pilots in particular. The present deliverable adds to this analysis by linking this analysis to legislation and legal principles.

As indicated, one of the legal sources (the GDPR) has not yet entered into application at the time of writing, and one (the SDGR) has not yet even been adopted. None the less, they have been taken into account due to their practical importance to the OOP: the GDPR will become applicable as of 25 May 2018 – i.e. in the course of the TOOP project – and the SDGR aims to provide the long-term legal underpinning of the OOP in the EU in the future. Therefore, they are critically important for defining the legal framework for the OOP. The potential impact of the proposed SDGR in particular will be described in greater detail in the following sections of this report.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Principles of the legal assessment framework and resulting requirements

Based on an analysis of the aforementioned legal sources, the following visual canvas containing the principles of the legal assessment framework can be provided:

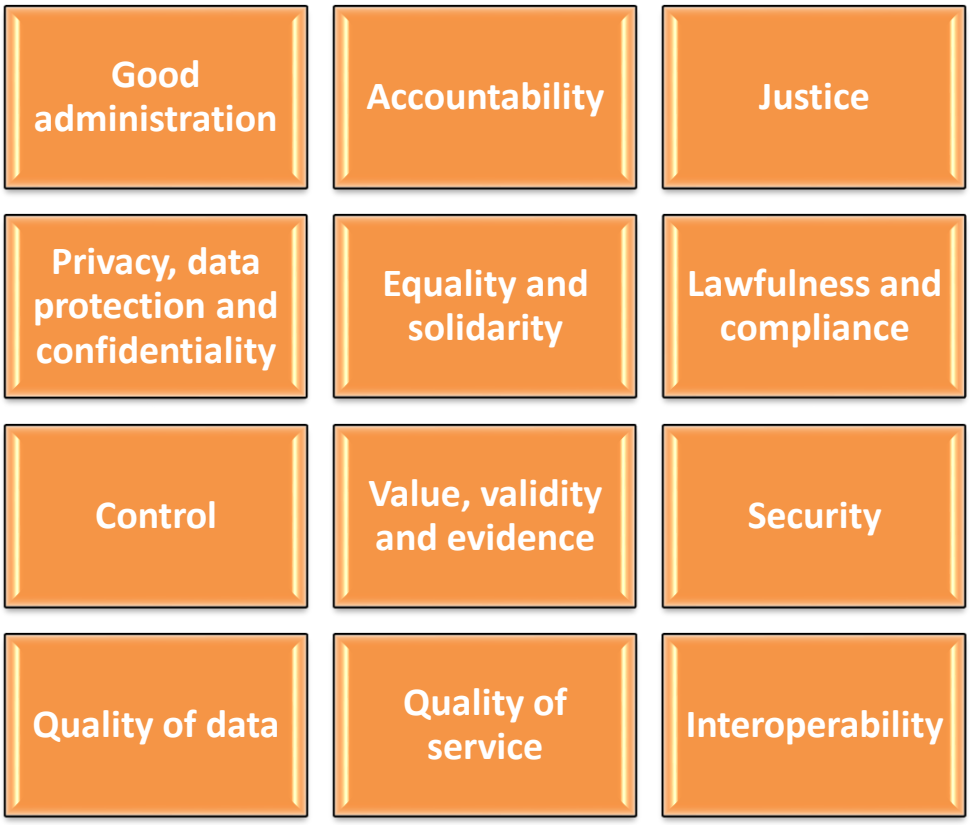

Figure 2: Canvas of the legal assessment framework

It should be emphasised that the legal assessment framework and the principles contained in the canvas above are intended to support the assessment of specific OOP use cases. It is emphatically not intended to provide a definition of the OOP (what does the OOP mean?), to determine its the scoping (which information should be made accessible via the OOP and under which conditions?), or whether the application of the OOP should be mandatory or not for any specific use case. These questions and others are answered within the TOOP project in TOOP D2.7 (2017), and more directly in TOOP D2.6 (2017). Outside of TOOP and likely after its termination, they will be answered in the finalised SDGR. The legal assessment framework thus assumes that these critical questions are already answered, and then assesses what the implications are for making the OOP work from a legal perspective in a specific use case.

The canvas above only provides a summary statement of the principles. The table below provides a more detailed description of what each principle means, and what the resulting requirements are. From a practical perspective, the table can be considered as a legal checklist to be applied to each OOP use case, allowing a determination of whether legal requirements have been satisfied. It should be noted that it is always somewhat arbitrary to decide whether a given principle should indeed be considered as separate or as a sub-element of another principle; it could e.g. be argued with some merit that the principle of accountability is a subsection of the broader principle of good

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

administration. However, the key element is that the requirements are defined appropriately, since these will be the criteria through which any OOP use case will be tested. The importance of the demarcation of principles or the allocation of requirements to one principle or another should not be overestimated.

Principles	Description and resulting requirements
Good administration	**Description**: the OOP must be implemented in a way that ensures that affairs are handled impartially, fairly and within a reasonable time. **Requirements**: • The OOP must be implemented in a way that ensures non-discrimination: evidence must be transferred on a neutral basis, without prejudicing any decisions that would be made by the receiving competent authority on the basis of the evidence. • The OOP must be implemented in a way that ensures transparency: the evidence to be transferred, the modalities of the transfer (specifically the duration of the accessibility of the evidence and the purposes of the exchange) and the categories of competent authorities involved must be clearly known to the persons concerned prior to the transfer. • If no evidence can be transferred, the competent authority must give reasons for this. • After the exchange, the receiving competent authority may only use the evidence for the purpose of the procedure for which the evidence was exchanged. as communicated to the persons benefiting from the OOP, excluding any use that is incompatible with the original purpose and any transfer to third parties (except where those third parties are required to achieve the communicated purposes). • The OOP must be implemented in a way that facilitates comprehension: without prejudice to the autonomy of the receiving competent authority, the person benefiting from the OOP should be able to receive information in relation to the evidence transfer process in his/her language of the Treaties.
Accountability	**Description**: the OOP must be implemented in a way that ensures that responsibilities are clearly allocated between each participant in the exchange of electronic evidence. **Requirements**: • The OOP must be implemented in a way that ensures that all participants are aware of their obligations, and that the persons relying on the OOP have the right to restitution of any damages caused by noncompliance with these obligations insofar as this is possible under applicable law (i.e. taking into account possible exemptions of liability that may apply to the competent authorities under their national laws).
Justice	**Description**: the OOP must be implemented in a way that ensures the right to recourse for the persons relying on the OOP, and that contains appropriate enforcement mechanisms. **Requirements**: • The OOP must be implemented in a way that safeguards the right of every person to be heard, before any individual measure which would affect him or her adversely is taken on the basis of evidence exchanged via the OOP.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

	• The OOP must therefore be implemented in a way that provides appropriate contact mechanisms for persons relying on the OOP towards all competent authorities involved as providers or as recipients of the evidence.

Privacy, data protection and confidentiality	**Description**: the OOP must be implemented in a way that safeguards the fundamental rights to privacy and data protection for natural persons, and respecting the legitimate interests of confidentiality and of professional and business secrecy.
	Requirements:
	• The evidence exchanged via the OOP may only be processed in accordance with applicable data protection law when it contains any personal data, notably the DPD, or as of 25 May 2018, the GDPR. This includes the principles of:
	  ○ lawfulness, fairness and transparency;
	  ○ purpose limitation;
	  ○ data minimisation;
	  ○ accuracy;
	  ○ storage limitation;
	  ○ integrity and confidentiality;
	  ○ accountability.
	• When the evidence exchanged via the OOP does not contain any personal data, the competent authorities must still ensure that appropriate measures are taken to ensure an appropriate level of confidentiality of the evidence exchanged. When there is a legitimate confidentiality concern, the same principles as under data protection law can be applied.

Equality and solidarity	**Description**: the OOP must be implemented in a way that protects the persons concerned against discrimination. **Requirements**: • The OOP must be implemented in a way that ensures non-discrimination: evidence must be transferred on a neutral basis, without prejudicing any decisions that would be made by the receiving competent authority on the basis of the evidence. • The OOP must be implemented in a way that ensures universal accessibility, including to persons with disabilities. Accessible support and communication mechanisms must be provided to ensure that such persons can receive comparable functionality as those persons benefiting from the OOP.
Lawfulness and compliance	**Description**: the OOP must be implemented in a way that ensures that evidence is only transferred if there is an adequate legal basis for this, and in compliance with any applicable legal requirements. **Requirements**: • Evidence may only be transferred under the OOP between competent authorities if there is a legal basis for this, either the consent of the persons concerned or a separate legal basis such as a legal obligation; • Evidence may only be transferred under the OOP between competent authorities if it has been determined that any pre-existing legal requirements (including sector or context specific legal requirements) are satisfied, including national authorisation procedures, legal agreements on usage restrictions, assurances with respect to security,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

	assurances or exclusions of liability, data or service quality arrangements, etc. During the course of the TOOP project, this will require a case by case assessment; after the entry into force of the SDGR this will likely be facilitated.
Control	**Description**: the implementation of the evidence exchange mechanism must contain appropriate controls to ensure that the evidence is relevant and to allow incidents to be detected and addressed. **Requirements**: • Prior to initiating any evidence exchange, the competent authorities participating in the exchange must verify the link between the identity of the person benefiting from the OOP and the corresponding evidence. • Appropriate audit and logging measures must be implemented to ensure that any exchange of evidence organised under the OOP can verified by competent authorities in case of disputes (including the identification of the sending and receiving competent authorities, the time of the exchange, and the integrity/authenticity of the exchanged data itself).
Value, validity and evidence	**Description**: the legal value and validity of any evidence exchanged under the OOP must be clear to all competent authorities participating in the exchange. **Requirements**: • There must be an understanding between the competent authorities on the legal value and validity of the evidence, including specifically whether the providing authority considers it to be authoritative (originating from and identical to information from an authoritative source or base register, i.e. any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity), or whether it can otherwise be assumed to be genuine. Ultimately, the receiving authority will decide whether the evidence is valid and appropriate for its purposes; but at a minimum the receiving authority must know the status of the information in the issuing authority's Member State.
Security	**Description**: the OOP must be implemented in a way that protects the exchanged evidence against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the evidence, thereby ensuring its integrity and authenticity. **Requirements**: • The competent authorities and any other participants in the evidence exchange mechanism must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: ○ the pseudonymisation and encryption of personal data; ○ the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; ○ the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; ○ a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

	• Incident response measures must be implemented to ensure that the exchange of compromised evidence is avoided and notified to recipients. Requirements under data protection law must at any rate be adhered to.
Quality of data	**Description**: the OOP must be implemented in a way that provides a clear shared understanding between all competent authorities on the quality of the exchanged evidence. **Requirements**: • A legal framework must exist that clarifies the obligations of the competent authorities in relation to the quality of the data, including any assurances of its accuracy, factual correctness, and timeliness of updates (which may take the form of legislation, SLAs, memoranda, or even nonbinding best efforts agreements; the requirement is that the understanding is clear). • A feedback mechanism must be in place that allows the persons involved to contact the competent authority at the source of the evidence to correct any inaccuracies.
Quality of service	**Description**: the OOP must be implemented in a way that provides a clear shared understanding between all competent authorities on the quality of the services for the exchange of evidence. **Requirements**: • A legal framework must exist that clarifies the obligations of the competent authorities in relation to the availability and responsiveness of the services (which may take the form of legislation, SLAs, memoranda, or even nonbinding best efforts agreements; the requirement is that the understanding is clear). • An evaluation mechanism must be in place that allows noncompliance with this framework to be detected and addressed when necessary.
Interoperability	**Description**: the OOP must be implemented in a way that ensures semantic and technical interoperability of the evidence exchanged under the OOP. **Requirements**: • Appropriate agreements must be in place with respect to the technical and semantic characteristics of the evidence to be exchanged between competent authorities, taking into account linguistic challenges and diversity of legal systems. Evidence should not be exchanged under the OOP if interoperability is not ensured.

Table 2: Legal assessment framework – principles and requirements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Summary of the legal assessment framework and the potential impact of the proposed SDGR

2.1.1. Comparison between the legal assessment framework and the proposed SDGR

The legal assessment framework above consists of a statement of principles that should be respected in all OOP use cases, based on a summary review of literature and key legislation, and the resulting testable requirements. While abstract, the legal assessment framework is intended to be used in practice as a systematic checklist to verify which legal challenges are likely to occur when implementing the OOP, and therefore what assurances should be provided by the legal solutions created around a specific use case.

Within the context of the TOOP project, a constraint is that there is no EU level legal basis yet for the OOP that would permit administrations to generically exchange digital evidence. This void would be filled by the proposed SDGR, which would provide a legal basis for the OOP in the use cases falling within its scope. The pilots of the TOOP project need to build on more narrowly tailored legal texts that provide a legal basis; as will be discussed in greater detail in chapter 3 below:

- For PA1, the exchange of evidence in response to the ESPD token is supported by the Public Procurement Directives;
- For PA2, the exchange of evidence is supported by the BRIS Directive and the BRIS Regulation;
- For PA3, the exchange of evidence is supported by multiple IMO Conventions and EU Directives 2010/65/EU and 2002/59/EC, in addition to Decision No 70/2008/EC.

In each of these cases, participants in the pilots therefore have a legal framework that address some of the legal requirements which are also defined by the legal assessment framework. As will have been obvious, most of the requirements in the framework are horizontal and could be satisfied in the same manner for any OOP use case. The principles of good administration, accountability, control and security are clear examples of requirements that are generic and which could be applied systematically across OOP use cases.

The proposal for a SDGR recognises this fact, since it aims to create a Single Digital Gateway that would be re-used in a highly similar manner for a well-defined but relatively broad (i.e. exhaustively enumerated but covering many areas of life and business activities) list of use cases.

The SDGR proposal envisages the creation of a 'technical system' for the electronic exchange of evidence between competent authorities in different Member States. Indeed, article 12 of the SDGR contains the following requirements in relation to this technical system:

> *(a) it shall enable the processing of requests for evidence to be exchanged;*
>
> *(b) it shall allow the transmission of evidence between competent authorities;*
>
> *(c) it shall allow the processing of the evidence by the receiving competent authority;*
>
> *(d) it shall ensure the confidentiality and integrity of the evidence;*
>
> *(e) it shall ensure that the user has the possibility to preview the evidence to be exchanged.*

The first three points relate more to the general description of the functionalities of the SDGR, but points (d) and (e) are encompassed in the principles of security and good administration of the legal assessment framework. Similarly, Article 12.6 of the SDGR requires that the "*evidence made available by a competent authority shall be strictly limited to what has been requested and shall only be used by the receiving authority for the purpose of the procedure for which the evidence was exchanged*"; this requirement too can be found in the principle of good administration which have been integrated in

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

the legal assessment framework above. The correspondence is of course not surprising, considering that the SDGR was taken into account during the drafting of the legal assessment framework.

There are none the less some differences between the principles in the TOOP framework above and the text of the SDGR. The scoping of the legal assessment framework is undeniably broader, and contains several details (e.g. in relation to quality of data and quality of service, or in relation to control mechanisms) which are not (yet) included in the SDGR; they may of course be integrated in the implementing acts that the Commission is permitted to adopt under Article 12.7 of the SDGR to set out the specifications of the technical system.

More importantly, the SDGR also contains a few principles that are not yet integrated into the legal assessment framework, notably:

- the requirement of an explicit request of the user before a competent authority can request evidence directly from another competent authority (Article 12.4);
- the obligation for competent authorities to make evidence available electronically provided that they issue evidence in electronic format within their own Member State (Article 12.5)
- a generic data minimisation principle requiring that "the evidence made available by a competent authority shall be strictly limited to what has been requested" (Article 12.6).

The choice was made not to integrate these requirements yet on the basis of the consideration that their application in practice for TOOP's use cases is not immediately obvious. Indeed, one of the objectives of TOOP is precisely to assess how and to what extent all of these principles can be observed in practice. Specifically:

- Some of the PAs work on the basis of a one-time authorisation from the user to retrieve evidence, which is granted to specific recipients. The latter can use this authorisation thereafter for an extended period of time to retrieve the evidence from the source. An explicit request for the user for each retrieval request is not imposed, nor is it necessary within TOOP that the user communicates directly with the competent authority. Arguably the SDGR does not require this either. However, TOOP also contains a few use cases where no requests are made by the users at all, but where the exchange of evidence is justified on different legal grounds. More explicitly, the maritime use case involves among other points evidence relating to crew members being exchanged, without any request or consent from the crew members. This is justified in that particular case since there is very specific legislation requiring exchange of the information (i.e. crew members have no choice on the matter, other than choosing not to become crew members), and due to the fact that the ship captain can control the exchange. TOOP thus has at least one use case which, to borrow terminology from the GDPR, is not based on consent of the user, but on a legal obligation enshrined in Member State and international law. Such cases do not seem to be envisaged by the SDGR, but are a part of TOOP; hence the absence of the user request requirement in the legal assessment framework within TOOP.
- No obligation for competent authorities to make evidence available is envisaged, since this is simply outside of the legal capabilities of a pilot project such as TOOP (although its inclusion in legislation such as the SDGR is obviously beneficial);
- The practical viability of a data minimisation duty is still untested; specifically, there is a concern that minimising data by applying a filter to existing electronic evidences may affect the possibility of authenticating it. In practical terms: making authentic electronic documents with standardised information available is challenging but feasible; requiring that some of the standardised information is filtered out if it is not relevant for a specific use case means that the new (filtered) evidence needs to be created on a case by case basis, with new measures required to ensure its authenticity and the ability to validate it. It is not clear if and how this

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

can be done within TOOP; provisionally the emphasis is on making existing information available 'as-is' (i.e. in unchanged, unfiltered form).

Part of these challenges arise also from the different scoping. TOOP addresses three pilot areas, which will be described in detail below. The proposed SDGR focuses exclusively on "the exchange of evidence for online procedures listed in Annex II and procedures provided for in Directives 2005/36/EC, 2006/123/EC, 2014/24/EU and 2014/25/EU"; i.e.:

- In Annex II:
  - Requesting a birth certificate
  - Applying for a study grant from a public institution
  - Registering for social security benefits
  - Requesting recognition of diploma
  - Registering a change of address
  - Requesting/renewing ID card or passport
  - Registering a motor vehicle
  - Claiming pension and preretirement benefits from public or semi-public schemes
  - General registration of business activity, excluding procedures concerning the constitution of companies or firms within the meaning of the second paragraph of Article 54 TFEU
  - Registration of an employer (a natural person) with public or semi-public pension and insurance schemes
  - Registration of employees with public or semi-public pension and insurance schemes
  - Notification to the social security schemes of the end of contract with an employee
  - Payment of social contributions for employees
- Directive 2005/36/EC, on the recognition of professional qualifications
- Directive 2006/123/EC, i.e. the Services Directive
- Directives 2014/24/EU and 2014/25/EU, i.e. the Public Procurement Directives

While there is a clear overlap notably with PA1 and PA2, PA3 (the maritime case) largely falls outside the scope of the objectives of the SDGR. Arguably, as will be examined in Chapter 3, the scoping of PA1 and PA2 in TOOP is also somewhat different from the vision of the SDGR.

For these reasons, it will be important to assess what the specificities of each PA are, and how TOOP can resolve them, taking into account the fact that the SDGR will likely still undergo evolutions and may not enter into application until after the completion of the TOOP project.

2.1.2. The EDPS Opinion on the proposed SDGR – addressing data protection challenges when implementing the OOP

One of the principles of the legal assessment framework used in TOOP is of course data protection: any implementation of the OOP in which personal data would be exchanged needs to comply with European data protection law. Within TOOP, the legal assessment framework examines this question from the perspective of the current Data Protection Directive and (more importantly given its application as of 25 May 2018) the General Data Protection Regulation. This implies that any application of the OOP must provide an answer on how the key principles of European data protection law are addressed, namely:

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimisation;
- accuracy;

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

- storage limitation;
- integrity and confidentiality;
- accountability.

The SDGR of course requires compliance with these principles as well. However, it does so in an arguably more stringent manner than the TOOP legal assessment framework. Article 29 contains a general obligation that "*processing of personal data within the framework of this Regulation by competent authorities must be in compliance with [Directive 95/46/EC] [Regulation (EU) 2016/679 of the European Parliament and of the Council]. Processing of personal data by the Commission within the framework of this Regulation, shall comply with the provisions of Regulation 00/0000 [new Regulation replacing Regulation 45/2001]*.". In such generic terms, the obligation corresponds to the TOOP legal assessment framework principle: the baseline requirement is compliance with data protection law.

However, Article 12 as written contains a set of requirements that implicitly and indirectly impact how data protection obligations must be implemented in practice. As already noted above:

- Article 12.2 (e) states that the technical system used for the exchange of electronic evidence "*shall ensure that the user has the possibility to preview the evidence to be exchanged*"; this can be considered a manifestation of the transparency principle.
- Article 12.4 states that competent authorities "*shall, upon an explicit request of the user, request evidence directly from competent authorities issuing evidence in other Member States through the technical system*"; the explicit request requirement can be considered an implementation of the lawfulness and fairness principles, including the treatment of data subject rights.
- Article 12.6 states that "*the evidence made available by a competent authority shall be strictly limited to what has been requested and shall only be used by the receiving authority for the purpose of the procedure for which the evidence was exchanged*"; these are arguable expressions of the data minimisation and purpose restriction principles.

The European Data Protection Supervisor (EDPS) published a specific opinion on the proposed SDGR on 1 August 2017[5], which largely approved of this approach while making a few additional suggestions.

Specifically, the EPDS welcomed the measures taken "*to ensure that individuals remain in control of their personal data, including by requiring 'an explicit request of the user' before any transfer of evidence between competent authorities and by offering the possibility for the user to 'preview' the evidence to be exchanged.*", and issued recommendations that emphasize the fact that the Proposal does not provide a legal basis for using the technical system for exchanging information for purposes other than those provided for in the four directives listed or otherwise foreseen under applicable EU or national law, and that the Proposal does not aim to provide a restriction on the principle of purpose limitation under the GDPR; as well as clarifying a range of issues relating to the practical implementation of user control. More generally, the Opinion stresses the importance of a clear legal basis for the processing; purpose limitation and data minimisation, and data subject rights.

The Opinion also analyses the lawfulness requirement of the processing of personal data in the context of the OOP, and notes that the three most relevant legal grounds for implementing the OOP principle are consent, legal obligation and processing in the context of a public task/official authority. It furthermore observes the stringent requirements around the consent concept, noting that lawfully given consent may not be possible in many cases where there is a risk of perceived coercion. "*As a*

[5] Opinion 8/2017 - EDPS Opinion on the proposal for a Regulation establishing a single digital gateway and the 'once-only' principle; see https://edps.europa.eu/sites/edp/files/publication/17-08-01_sdg_opinion_en.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

general rule of thumb, for the case of any recurring and structural data sharing, the EDPS recommends -in order to ensure legal certainty- that whenever possible, further processing of personal data based on the once-only principle be specified in a legislative instrument."

Thus, consent requirements are not integral to ensuring compliance with data protection law in the context of the once-only principle. None the less, the SDGR proposal certainly goes in this direction: the requirement of review and explicit request (as enshrined in the proposal) could be interpreted as a consent requirement for each transfer. The EDPS seems to support this view, by suggesting the improvement that "*a request can only be considered explicit if it contains a freely given, specific, informed and unambiguous indication of the individual's wishes to have the relevant information exchanged, either by statement or affirmative action*". Other suggested improvements are clarifications on how specific the request should be, the obligation to clarify the consequences of withholding a request, and making the request revocable. This would seem to make the 'request' concept virtually indistinguishable from a consent requirement under data protection law, which has identical underpinnings.

Limiting the implementation of the once-only principle to cases based on request is a legitimate policy choice, but it also has two potential negative implications that TOOP will encounter. Firstly, the requirement of requesting and previewing makes it impossible to implement OOP use cases in which the lawfulness of an exchange is based on law rather than consent. As will be explained in greater detail in the sections below, TOOP has one use case where ship crew member certificates would be exchanged from the crew member's port authority to controlling authorities in destination ports. Implementing a request and preview requirement makes this process unmanageable: it would imply that each crew member would need to agree to the presentation of its certificates before entering any port. It would likely also be unlawful: as the EPDS rightly argues, such a request would not be freely made, since the crew member would be under the authority of its captain and therefor clearly subject to possible coercion. Most importantly, a request is arguably useless, since the transfer of information is justified by international treaties, EU directives and national laws. None the less, implementing a request and preview duty makes it impossible to treat this use case via a generic OOP technical system.

Secondly, the current implementation makes repeated exchanges of digital evidence impossible, even if this has a legal basis or has been requested by the end user. By way of an example that TOOP endeavours to pilot: an end user could authorise a public authority to repeatedly access information from a business register, e.g. to show its continued compliance with procurement requirements, for a predefined period which could be terminated by the end user. However, the currently proposed draft SDGR does not enable this, since the request is required for *each* transfer.

The EDPS furthermore strengthened the perspective that the preview should also be available for each transfer, by suggesting that "*that the user is offered a possibility of preview in a timely manner before the evidence is made accessible to the recipient; […] this can be done, for example, by inserting the words at the end of the sentence in Article 12(2)(e): 'before it is made accessible to the requesting authority, and may withdraw the request at any time')*".

If these rules as construed as requiring a request and a preview per individual transfer, this would make repeated access to the data impractical, since the end user would need to preview and request it each time, creating a burden for the end user (who may have no objection against the repeated accesses) and for the requesting authority (who can only get the data by contacting the end user each time and asking for a new request and preview). This could be solved by clarifying that, when data transfers are based on a request (which, as argued above, should not be the sole option if all TOOP use cases are to be covered by the SDGR), the request may pertain to repeated access to the data, provided that the request is then of course revocable, and that the end user can choose at any time to preview the data that a receiving party would get access to.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

In summary, while TOOP of course fully recognises the critical importance of compliance with data protection law, there is a concern that the operationalisation of these principles in the SDGR proposal as written may exclude a few once-only use cases, without necessarily creating a data protection benefit. Specifically, the request and preview requirements *de facto* may result in a consent requirement, eliminating exchanges that are based on legal obligations and processing in the context of a public task/official authority. The EDPS Opinion explicitly notes that these would be viable from a data protection perspective too, but the current approach of the SDGR seems to exclude them. In addition, there is a concern that the current phrasing of the SDGR requires a request and preview per transfer, which would make a request to permit repeated access to digital evidence impossible. A broader approach that focuses more on all three grounds of exchange (request, legal obligation and public task, rather than requests only) would permit more use cases to be supported.

Doing so would also address a second potential challenge. The EDPS rightly observes that the lawfulness of the technical system (given a legal basis by the SDGR) does not justify all OOP evidence exchanges as such; the latter require a separate legal basis. The current SDGR proposal addresses this issue on the one hand by introducing a request requirement (which *de facto* seems indistinguishable from consent requirement as currently approached), and on the other by explicitly listing four Directives and an Annex II of use cases for which the technical system might be used.

Beyond the challenge that the EPDS highlighted in its opinion, namely that the use cases of Annex II are possibly too abstract to be able to understand them correctly, there is a second problem, namely that cases for which a clear legal basis exists are still excluded from using the technical system if they don't fall within the closed list. The maritime use case of TOOP would be a primary example of a victim: the legal basis exists and all possible measures to safeguard data protection could be implemented, but it is barred from using the SDGR technical system as it is not explicitly listed as a use case. Generalising the legitimacy requirements by stating that the use of the technical system must be based on a request, legal obligation or public task would result in the possibility of more use cases being integrated.

The statements above should not be misconstrued as a criticism of the SDGR proposal or of the EDPS Opinion, but rather as an expression of concern that some of the pilots of TOOP may not be continued after the project's termination under the SDGR, unless some clarifications are made.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

3. Legal assessment of the three pilot areas

Chapter 2 defined the legal assessment framework, containing crucial legal principles and the resulting requirements. In this chapter, a legal assessment of the three pilot areas is done, firstly by identifying any specific legal and policy requirements that are unique to the PAs, and secondly by applying the legal assessment framework to the PAs. The outcome is a concise statement of legal challenges which are specific to each pilot area.

General approach to the assessment of the pilot areas

In order to conduct the legal assessment of the three PAs in a coherent and consistent manner, each section below will consist of three parts:

- The identification of applicable legislation for that specific PA (i.e. ignoring horizontal requirements that are comprised in the legal assessment framework) and the identification of resulting legal challenges;
- The application of the legal assessment framework to determine which requirements are likely to cause challenges in practice;
- A summary statement of legal challenges which are specific to the pilot area.

It should be noted that the sections have been drafted taking into account discussions with pilot leaders for each PA, in order to ensure that the analysis is supported in reality. Furthermore, the identification of requirements was also supported by the use of a questionnaire[6] that was transmitted to any Member State participating in any of the pilots, so that there national legal and procedural requirements could be pragmatically identified. This is necessary because, within the context of a pilot project like TOOP, it would not be feasible to examine national laws comprehensively on a case by case basis. Therefore, the questionnaire was used to identify any national legal concerns and requirements without having to revert to national level legal studies.

Cross-border e-Services for Business Mobility Pilot (PA1)

3.1.1. Summary description of PA1 and identification of PA1 specific legislation

The Cross-border e-Services for Business Mobility pilot includes three motivational scenarios[7]:

- European Single Procurement Document (ESPD), in which this self-declaration document is used by a company as a token towards a third party, authorising that third party to access information in relation to the company from designated sources such as business registers, particularly in the context of public procurement.
- Mandate consumption, in which interested third parties can pull information about legal representation powers for legal entities directly from business registers with the authorisation of the legal entity;
- Licenses and Permissions, in which interested third parties can determine existing professional qualifications and competences against the backdrop of the Services Directive and the Professional Qualifications Directive.

For the first of the three motivational scenarios, the European Single Procurement Document (ESPD) is, from a legal perspective, the critical enabler. The ESPD already exists and has a clear legal framework

[6] Available as Appendix I in TOOP Deliverable D2.7 (2017)

[7] TOOP Alignment workshop WP2 / WP3. WP3.1 Cross-border e-Services for Business Mobility. 18 Apr 2017. Antonis Stasis, Loukia Demiri

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

via the Directives 2014/24/EU (Article 59) and 2014/25/EU, i.e. the Public Procurement Directives. The ESPD is currently conceived as a regulated and standardised self-declaration form in public procurements. The ESPD essentially solves an evidentiary problem: without an ESPD, companies can be required to submit various documents to prove that they fulfil the exclusion and selection criteria of a tender (e.g. that they have paid taxes and have not been convicted of criminal activity)[8]. The ESPD alleviates that problem: as a self-declaration form, economic operators can participate in procurements using only the form, and actual evidentiary documents will only have to be provided by the winner of the tender.

There are currently four possibilities of using the ESPD[9]:

Through the free ESPD service provided by the European Commission.

- Through the free ESPD data model, which enables integration of the ESPD service into national e-procurement solutions/pre-qualification services.
- Through the open source version of the free ESPD service, which can be adjusted to take into account national needs.
- Through the Virtual Company Dossier (VCD), which allows the buyers to handle the ESPDs (like the first option) and the tenderers to benefit from an automated filling-in of the ESPD.

However, PA1 aims to extend the functionality of the ESPD by using it as an authorisation from an economic operator to obtain information directly from a source register. The application is in line with the existing vision and use of the ESPD: Article 59 of Directive 2014/24/EU indeed states that the ESPD must *„identify the public authority or third party responsible for establishing the supporting documents and contain a formal statement to the effect that the economic operator will be able, upon request and without delay, to provide those supporting documents.*

Where the contracting authority can obtain the supporting documents directly by accessing a database pursuant to paragraph 5, the EPSD shall also contain the information required for this purpose, such as the internet address of the database, any identification data and, where applicable, the necessary declaration of consent. [...] Economic operators shall not be required to submit supporting documents or other documentary evidence where and in so far as the contracting authority has the possibility of obtaining the certificates or the relevant information directly by accessing a national database in any Member State that is available free of charge, such as a national procurement register, a virtual company dossier, an electronic document storage system or a prequalification system.

[...] Member States shall ensure that databases which contain relevant information on economic operators and which may be consulted by their contracting authorities may also be consulted, under the same conditions, by contracting authorities of other Member States.

Member States shall make available and up-to-date in e-Certis a complete list of databases containing relevant information on economic operators which can be consulted by contracting authorities from other Member States. Upon request, Member States shall communicate to other Member States any information related to the databases referred to in this Article".

The ESPD therefore would allow the public authority to request the data directly from the source registers. The ESPD no longer functions just as a self-declaration; it essentially becomes a 'key' or 'token' that allows the contracting authority to pull data directly from certain sources.

[8] See http://ec.europa.eu/growth/single-market/public-procurement/e-procurement/espd/

[9] As also described on http://ec.europa.eu/growth/single-market/public-procurement/e-procurement/espd/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

The second and third motivational scenarios (Mandate consumption[10] and Licenses/permissions) are more traditional applications of the OOP. The former relates to the ability of interested third parties to pull information about legal representation powers for legal entities directly from business registers (comparable to PA2 as will be discussed below), and the latter to the determination of existing professional qualifications and competences against the backdrop of the Services Directive and the Professional Qualifications Directive. In that sense, they are more application neutral: whereas scenario 1 is tied to public procurements, scenarios 2 and 3 are open-ended.

The importance of PA1 in the context of the proposed SDGR is clear: for the ESPD motivational scenario, the draft SDGR states that the "*European Single Procurement Document (ESPD) is a self-declaration of compliance with requirements related to public procurement procedures. Its electronic version has the potential to become a key building block of the implementation of the once-only-principle in public procurement.*" For the License and Mandate motivational scenarios, both the Services Directive and the Professional Qualifications Directive are listed as topics in scope of Article 12.

PA1 is also highly relevant because the existing legal framework does not offer a comprehensive legal basis to directly implement the three motivational scenarios; while the use of the ESPD as envisaged in scenario 1 is more directly covered, access by third parties to business registers and registers of professional qualifications and competences is not as clearly defined. In the absence of encompassing legislation (i.e. until the entry into force of a finalised SDGR and its implementation), TOOP will need to create a contractual framework that satisfies the legal needs of the motivational scenarios of PA1.

It is particularly worth noting that the voluntary agreement will be needed from data providers (like business registers) to participate in some of the motivational scenarios, as there are no laws forcing them to provide the required information in all cases. PA1 of course does not operate in a vacuum: a legal basis exists through the Public Procurement Directives, the Services Directive, the Professional Qualifications Directive and the BRIS Directive. However, none of these ensure the accessibility and availability of business register data to third parties as envisaged by PA1, including the availability of data in a machine processable form.

Finally, it should also be remembered that certain details on the scoping and deployment of PA1 are still subject to evolution. The ESPD in particular could be used 'as is', in its current format and following current standards; or alternatively as a blank document that contains no substantive information but which can be used in conjunction with eCertis 2.0 to merely determine whether requirements for any particular procurement have been complied with (a green light versus red light), that would be more effective from a confidentiality / privacy protection perspective.

3.1.2. Application of the legal assessment framework to PA1

Having summarily described the specific legislation that applies to PA1, a more systematic assessment of legal challenges will be done using the legal assessment framework. In the table below, the requirements of the legal assessment framework will be applied to PA1, indicating whether there are any unique challenges or concerns (beyond those that would be required for any OOP use case).

[10] Referring in this context to a scenario where information which may or may not be contained in business registers is made available to relying parties. By way of an example: official representatives of a company (as registered with the business register) often delegate certain tasks, such as tax declaration, to another person; the objective is to make such mandates available to third parties.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Requirement of the legal assessment framework	Impacts which are specific to PA1 (if any)
Good administration requirements: • The OOP must be implemented in a way that ensures non-discrimination: evidence must be transferred on a neutral basis, without prejudicing any decisions that would be made by the receiving competent authority on the basis of the evidence. • The OOP must be implemented in a way that ensures transparency: the evidence to be transferred, the modalities of the transfer (specifically the duration of the accessibility of the evidence and the purposes of the exchange) and the categories of competent authorities involved must be clearly known to the persons concerned prior to the transfer. • If no evidence can be transferred, the competent authority must give reasons for this. • After the exchange, the receiving competent authority may only use the evidence for the purpose of the procedure for which the evidence was exchanged. as communicated to the persons benefiting from the OOP, excluding any use that is incompatible with the original purpose and any transfer to third parties (except where those third parties are required to achieve the communicated purposes). • The OOP must be implemented in a way that facilitates comprehension: without prejudice to the autonomy of the receiving competent authority, the person benefiting from the OOP should be able to receive information in relation to the evidence transfer process in his/her language of the Treaties.	Impacts: • Transparency: the categories of recipients of evidence must be identified to the user. This will require a clear delineation of permissible requesting parties. Likely starting point will be: ○ For the ESPD: contracting authorities ○ For the License: public authorities in general ○ For the Mandates: public authorities in general • It is likely that the ESPD scenario will be implemented via intermediaries, i.e. third parties that obtain an ESPD and conduct a check against know registers, functionally comparable to prequalification services that already exist in public procurements, e.g. in construction procurements. This would simplify the model, as the number of prequalification service providers is lower than the number of contracting authorities.
Accountability requirements: • The OOP must be implemented in a way that ensures that all participants are aware of their obligations, and that the persons relying on the OOP have the right to restitution of any damages caused by noncompliance with these obligations insofar as this is possible under applicable law (i.e. taking into account possible exemptions of liability that may apply to the competent authorities under their national laws).	Impacts: • None which are unique to PA1

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Justice requirements: • The OOP must be implemented in a way that safeguards the right of every person to be heard, before any individual measure which would affect him or her adversely is taken on the basis of evidence exchanged via the OOP. • The OOP must therefore be implemented in a way that provides appropriate contact mechanisms for persons relying on the OOP towards all competent authorities involved as providers or as recipients of the evidence.	Impacts: • None which are unique to PA1

Privacy, data protection and confidentiality requirements:
• The evidence exchanged via the OOP may only be processed in accordance with applicable data protection law when it contains any personal data, notably the DPD, or as of 25 May 2018, the GDPR. This includes the principles of:
  ○ lawfulness, fairness and transparency;
  ○ purpose limitation;
  ○ data minimisation;
  ○ accuracy;
  ○ storage limitation;
  ○ integrity and confidentiality;
  ○ accountability.
• When the evidence exchanged via the OOP does not contain any personal data, the competent authorities must still ensure that appropriate measures are taken to ensure an appropriate level of confidentiality of the evidence exchanged. When there is a legitimate confidentiality concern, the same principles as under data protection law can be applied.
	Impacts:
	• Personal data protection legislation will need to be complied with, since personal data can be included in the ESPD scenario, and will inevitably be included in the Mandates and License scenarios. This implies the creation of a legal framework that ensures compliance with the stated principles.
	• Purpose limitation, data minimisation and storage limitation are key concerns. In practice, any authorisation to access source registers (such as the ESPD) will need to be limited in time. Either the ESPD must be revocable, or it must be bound to a specific procurement (so that the ESPD can no longer be used to access information after the completion of the procurement).

Equality and solidarity requirements: • The OOP must be implemented in a way that ensures non-discrimination: evidence must be transferred on a neutral basis,	Impacts: • None which are unique to PA1

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

without prejudicing any decisions that would be made by the receiving competent authority on the basis of the evidence. • The OOP must be implemented in a way that ensures universal accessibility, including to persons with disabilities. Accessible support and communication mechanisms must be provided to ensure that such persons can receive comparable functionality as those persons benefiting from the OOP.	
Lawfulness and compliance requirements: • Evidence may only be transferred under the OOP between competent authorities if there is a legal basis for this, either the consent of the persons concerned or a separate legal basis such as a legal obligation; • Evidence may only be transferred under the OOP between competent authorities if it has been determined that any pre-existing legal requirements (including sector or context specific legal requirements) are satisfied, including national authorisation procedures, legal agreements on usage restrictions, assurances with respect to security, assurances or exclusions of liability, data or service quality arrangements, etc. During the course of the TOOP project, this will require a case by case assessment; after the entry into force of the SDGR this will likely be facilitated.	Impacts: • The legal basis is relatively clearly demarcated: the consent of the person concerned is provided in each case. Furthermore, competent authorities will exchange information on the basis of the Public Procurement Directives, Services Directive, Professional Qualifications Directive, and BRIS Directive. The key element will in each case be the individual consent. • There are clear definitions of the contents and format of the ESPD. Insofar as these are redrafted (e.g. in order to allow their use under eCertis 2.0), new profiles need to be agreed upon.
Control requirements: • Prior to initiating any evidence exchange, the competent authorities participating in the exchange must verify the link between the identity of the person benefiting from the OOP and the corresponding evidence. • Appropriate audit and logging measures must be implemented to ensure that any exchange of evidence organised under the OOP can verified by competent authorities in case of disputes (including the identification of the sending and receiving competent authorities, the time of the exchange, and the integrity/authenticity of the exchanged data itself).	Impacts: • For the ESPD, there are already tools available to create it which need to be reused. As the ESPD already exists and is operational, the link between identity and evidence is already sufficiently substantial from a legal perspective. For the ESPD motivational scenario, there is therefore no need to align further on identification, authentication or signature requirements. The Mandate and License scenarios on the other hand may require alignment with the eIDAS Regulation. • Logging mechanisms must be implemented to ensure that evidence exchanges can be verified afterwards. This is especially important in PA1 since some of the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

	information made accessible via the ESPD can be confidential or private (e.g. blank criminal record, payment of taxes and social security).
Value, validity and evidence requirements: • There must be an agreement between the competent authorities on the legal value and validity of the evidence, including specifically whether it can be considered authoritative (originating from and identical to information from an authoritative source or base register, i.e. any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity), or whether it can otherwise be assumed to be genuine.	Impacts: • Less complex for PA1 than for many other OOP use cases, since the legal value and validity of the evidence is clearly regulated.
Security requirements: • The competent authorities and any other participants in the evidence exchange mechanism must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: ○ the pseudonymisation and encryption of personal data; ○ the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; ○ the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; ○ a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. • Incident response measures must be implemented to ensure that the exchange of compromised evidence is avoided and notified to recipients. Requirements under data protection law must at any rate be adhered to.	Impacts: • None which are unique to PA1
Quality of data requirements:	Impacts:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

• A legal framework must exist that clarifies the obligations of the competent authorities in relation to the quality of the data, including any assurances of its accuracy, factual correctness, and timeliness of updates (which may take the form of legislation, SLAs, memoranda, or even nonbinding best efforts agreements; the requirement is that the understanding is clear). • A feedback mechanism must be in place that allows the persons involved to contact the competent authority at the source of the evidence to correct any inaccuracies.	• Less complex for PA1 than for many other OOP use cases, since the content and quality of the evidence is clearly regulated.
Quality of service requirements: • A legal framework must exist that clarifies the obligations of the competent authorities in relation to the availability and responsiveness of the services (which may take the form of legislation, SLAs, memoranda, or even nonbinding best efforts agreements; the requirement is that the understanding is clear). • An evaluation mechanism must be in place that allows noncompliance with this framework to be detected and addressed when necessary.	Impacts: • Availability and responsiveness will require commitments from data sources, which are presently not under any obligation of continuous availability of their services. This can be relevant for all three motivational scenarios, but perhaps more so for the Mandate scenario where instantaneous confirmation of a legal mandate may be expected.
Interoperability requirements: • Appropriate agreements must be in place with respect to the technical and semantic characteristics of the evidence to be exchanged between competent authorities, taking into account linguistic challenges and diversity of legal systems. Evidence should not be exchanged under the OOP if interoperability is not ensured.	Impacts: • Limited challenges for the ESPD motivational scenario where there is significant experience with this problem or for the License motivational scenario which is governed by a specific legal framework. More significant challenges for the Mandate scenario since mandates are not harmonised/standardised for most legal entities in the EU. However, if the scoping is focused on confirming the name and nature of the mandate (rather than on ensuring that the name and nature are perfectly understood and interpreted), challenges are limited.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

3.1.3. Summary statement of legal challenges for PA1

As the overview above has shown, there are several specific legal challenges in implementing PA1:

- Scoping: it must be clearly delineated which competent authorities will be able to gain access to information in source registers. All motivational scenarios are predicated on the prior consent of the person concerned, so this can be built in as a safeguard.
- Legal recognition of the ESPD 'token' by third parties for motivational scenario 1, notably the competent authorities that would be providing evidence in response to the ESPD token. This is supported by the Public Procurement Directives, but requires operationalisation to ensure that competent authorities respond to the ESPD token.
- In motivational scenarios 2 and 3 (Licences and Permissions, Basic company data and Legal Person Mandates), there must similarly be a recognition by information providers of the legal request made by the end user to provide information from a business register (or other data source) directly to the authority envisaged (typically but not exclusively the Point of Single Contact as designated under the Services Directive).
- Ensuring the traceability and logging of any use of the token: breaches must be identifiable so that unlawful access can be detected and addressed.
- Revocability: the 'token' may not have an unlimited duration since that would cause confidentiality / privacy concerns. This can be done either by specifying a standardised expiration date for the ESPDs, or by allowing explicit revocation. Standardised expiration dates would likely be more viable.

The principal solution approach would be to establish a contractual framework in which the data providers agree to provide the specified evidence on the basis of the token, including shared policies on the requirements of the legal assessment framework.

Updating Connected Company Data Pilot (PA2)

3.1.4. Summary description of PA2 and identification of PA2 specific legislation

The Updating Connected Company Data Pilot implements an event notification service from the Business Registers towards any public administration at the European level. This could reduce the burden for the companies, ensuring at the same time the administrations of any MS of the correct, timely and complete update of the relevant company data.

The pilot will function in two modes, which can be considered as separate motivational scenarios. Public authorities can either (1) subscribe to receive updated information from business registers (a push model) or (2) get access to data on demand (a pull model). The pilot is thus oriented towards public sector users (not to private companies or individuals), although the requirements for accessibility of the evidence from the business registers may be conditional upon a payment (i.e. from the perspective of the operators of the business registers, the pilots can be commercial services).

The primary pre-existing legal framework is of course the BRIS Directive 2012/17/EC[11] and the BRIS Implementing Regulation[12], supported architecturally by the BRIS building block.

Through the BRIS Directive, all EU Member States are required to enable electronic communication between business registers and transmit certain information to individual users in a standardised way, by means of identical content and interoperable technologies, throughout the European Union. The

[11] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012L0017

[12] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2015.144.01.0001.01.ENG

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

system of interconnection of registers shall be composed of the registers of Member States, a central platform, and one or more access portals. The European e-Justice Portal – through the Find-a-company service[13] - will serve as the European electronic access point.

Under the Directive, the registers must make the following information available free of charge through the interconnection:

- the name and legal form of the company;
- the registered office of the company and the Member State where it is registered; and
- the registration number of the company; and
- information on winding-up or insolvency proceedings.

The new Directive also stipulates that the European Commission may, by means of implementing acts, specify the technical specification defining among others: the structure of the standard message format for the purpose of the exchange of information between the registers, the platform and the portal; and the technical specification defining the structure and use of the unique identifier for communication between registers. This has been done via the BRIS Implementing Regulation and the Core Business Vocabulary v1.00.

It should be noted that the BRIS Regulation provides for many of the details required for the implementation of PA2, including many of the requirements contained in the legal assessment framework. This includes security standards, interoperability requirements, and even requirements for the availability of services (requiring a service time frame of 24/7days, with an availability rate of the system of at least 98 % excluding scheduled maintenance, and rules for scheduling maintenance). While still high level, these can be re-used for PA2 as well.

The existence of the BRIS and its core functionality is therefore already clearly regulated and operational in at least some Member States via the aforementioned eJustice portal, including a definition of technical aspects, interoperability challenges and the availability of free information. However, PA2 adds several components to this, namely the subscription based push model (not foreseen under the Directive), and a pull model that can include additional information beyond the aforementioned points that fall under the mandatory scope of the BRIS Directive. This is possible: the BRIS Directive explicitly allows Member States “to establish one or more optional access points, which may have an impact on the use and operation of the platform”, subject to notification to the Commission. PA2 could be construed as an instantiation of this right, which could permit its long-term sustainability.

3.1.5. Application of the legal assessment framework to PA2

Having summarily described the specific legislation that applies to PA2, a more systematic assessment of legal challenges will be done using the legal assessment framework. In the table below, the requirements of the legal assessment framework will be applied to PA2, indicating whether there are any unique challenges or concerns (beyond those that would be required for any OOP use case).

[13] https://e-justice.europa.eu/content_find_a_company-489-en.do?m=1.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

Requirement of the legal assessment framework	Impacts which are specific to PA2 (if any)
Good administration requirements: • The OOP must be implemented in a way that ensures non-discrimination: evidence must be transferred on a neutral basis, without prejudicing any decisions that would be made by the receiving competent authority on the basis of the evidence. • The OOP must be implemented in a way that ensures transparency: the evidence to be transferred, the modalities of the transfer (specifically the duration of the accessibility of the evidence and the purposes of the exchange) and the categories of competent authorities involved must be clearly known to the persons concerned prior to the transfer. • If no evidence can be transferred, the competent authority must give reasons for this. • After the exchange, the receiving competent authority may only use the evidence for the purpose of the procedure for which the evidence was exchanged. as communicated to the persons benefiting from the OOP, excluding any use that is incompatible with the original purpose and any transfer to third parties (except where those third parties are required to achieve the communicated purposes). • The OOP must be implemented in a way that facilitates comprehension: without prejudice to the autonomy of the receiving competent authority, the person benefiting from the OOP should be able to receive information in relation to the evidence transfer process in his/her language of the Treaties.	Impacts: • The purpose restriction requirement can be challenging: access to business register data is application neutral (in the sense that the usage cannot be verified or controlled by the business register operators). This can be addressed by specifying that obtained information may only be used lawfully and in accordance with applicable law. While generic, this is in line with the general publicity objectives of the BRIS Directive. • Transparency: it must be ensured that public authorities cannot push/pull data from a business register without the awareness of the entities involved. This can be implemented via a transparency requirement in which the public authority must inform an entity that it will use PA2 services (including to what extent and for how long, and termination modalities). This is necessary because, unlike the publicly accessible data that can be obtained via the eJustice Portal, the PA2 has no other legal basis.
Accountability requirements: • The OOP must be implemented in a way that ensures that all participants are aware of their obligations, and that the persons relying on the OOP have the right to restitution of any damages caused by	Impacts: • None which are unique to PA2

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

noncompliance with these obligations insofar as this is possible under applicable law (i.e. taking into account possible exemptions of liability that may apply to the competent authorities under their national laws).	
Justice requirements: • The OOP must be implemented in a way that safeguards the right of every person to be heard, before any individual measure which would affect him or her adversely is taken on the basis of evidence exchanged via the OOP. • The OOP must therefore be implemented in a way that provides appropriate contact mechanisms for persons relying on the OOP towards all competent authorities involved as providers or as recipients of the evidence.	Impacts: • None which are unique to PA2.

Privacy, data protection and confidentiality requirements:
• The evidence exchanged via the OOP may only be processed in accordance with applicable data protection law when it contains any personal data, notably the DPD, or as of 25 May 2018, the GDPR. This includes the principles of:
  ○ lawfulness, fairness and transparency;
  ○ purpose limitation;
  ○ data minimisation;
  ○ accuracy;
  ○ storage limitation;
  ○ integrity and confidentiality;
  ○ accountability.
• When the evidence exchanged via the OOP does not contain any personal data, the competent authorities must still ensure that appropriate measures are taken to ensure an appropriate level of confidentiality of the evidence exchanged. When there is a legitimate confidentiality concern, the same principles as under data protection law can be applied.
	Impacts:
	• None which are unique to PA2. Compliance with data protection law is already legally required under the BRIS Directive; retaining this obligation is adequate.

Equality and solidarity requirements:	Impacts:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

• The OOP must be implemented in a way that ensures non-discrimination: evidence must be transferred on a neutral basis, without prejudicing any decisions that would be made by the receiving competent authority on the basis of the evidence. • The OOP must be implemented in a way that ensures universal accessibility, including to persons with disabilities. Accessible support and communication mechanisms must be provided to ensure that such persons can receive comparable functionality as those persons benefiting from the OOP.	• None which are unique to PA2
Lawfulness and compliance requirements: • Evidence may only be transferred under the OOP between competent authorities if there is a legal basis for this, either the consent of the persons concerned or a separate legal basis such as a legal obligation; • Evidence may only be transferred under the OOP between competent authorities if it has been determined that any pre-existing legal requirements (including sector or context specific legal requirements) are satisfied, including national authorisation procedures, legal agreements on usage restrictions, assurances with respect to security, assurances or exclusions of liability, data or service quality arrangements, etc. During the course of the TOOP project, this will require a case by case assessment; after the entry into force of the SDGR this will likely be facilitated.	Impacts: • The legal basis for PA2 (unlike for the BRIS services provided by the eJustice Portal which finds its justification in the BRIS Directive and the BRIS Implementing Regulation) will be the consent of the businesses involved. As will be explained below, a federation agreement will need to be concluded between the public authorities accessing the business registers and the operators of the business registers; this will specify that the public authorities will not avail themselves of the PA2 services without the consent of the entities involved.
Control requirements: • Prior to initiating any evidence exchange, the competent authorities participating in the exchange must verify the link between the identity of the person benefiting from the OOP and the corresponding evidence. • Appropriate audit and logging measures must be implemented to ensure that any exchange of evidence organised under the OOP can verified by competent authorities in case of disputes (including the identification of the sending and receiving competent authorities, the	Impacts: • For PA2 this is in practice resolved through the systematic use of the EUID (European Unique Identifier), as already envisaged by the BRIS Directive and BRIS Regulation. This system is appropriate for the BRIS service on the eJustice Portal, and would serve the exact same purpose for PA2.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

time of the exchange, and the integrity/authenticity of the exchanged data itself).	
Value, validity and evidence requirements: • There must be an agreement between the competent authorities on the legal value and validity of the evidence, including specifically whether it can be considered authoritative (originating from and identical to information from an authoritative source or base register, i.e. any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity), or whether it can otherwise be assumed to be genuine.	Impacts: • This can in practice draw on the BRIS Directive and the BRIS Regulation, since the data is substantively identical.

Security requirements:
• The competent authorities and any other participants in the evidence exchange mechanism must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
  ○ the pseudonymisation and encryption of personal data;
  ○ the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  ○ the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
  ○ a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
• Incident response measures must be implemented to ensure that the exchange of compromised evidence is avoided and notified to recipients. Requirements under data protection law must at any rate be adhered to.
	Impacts:
	• This can in practice draw on the BRIS Directive and the BRIS Regulation, which defines (very high level) security requirements.

Quality of data requirements:	Impacts:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

• A legal framework must exist that clarifies the obligations of the competent authorities in relation to the quality of the data, including any assurances of its accuracy, factual correctness, and timeliness of updates (which may take the form of legislation, SLAs, memoranda, or even nonbinding best efforts agreements; the requirement is that the understanding is clear). • A feedback mechanism must be in place that allows the persons involved to contact the competent authority at the source of the evidence to correct any inaccuracies.	• This can in practice draw on the BRIS Directive and the BRIS Regulation, since the data is substantively identical.
Quality of service requirements: • A legal framework must exist that clarifies the obligations of the competent authorities in relation to the availability and responsiveness of the services (which may take the form of legislation, SLAs, memoranda, or even nonbinding best efforts agreements; the requirement is that the understanding is clear). • An evaluation mechanism must be in place that allows noncompliance with this framework to be detected and addressed when necessary.	Impacts: • This can be based on the BRIS Regulation, which contains requirements for the availability of services (requiring a service time frame of 24/7days, with an availability rate of the system of at least 98 % excluding scheduled maintenance, and rules for scheduling maintenance). While still high level, these can be re-used for PA2.
Interoperability requirements: • Appropriate agreements must be in place with respect to the technical and semantic characteristics of the evidence to be exchanged between competent authorities, taking into account linguistic challenges and diversity of legal systems. Evidence should not be exchanged under the OOP if interoperability is not ensured.	Impacts: • This can in practice draw on the BRIS Directive and the BRIS Regulation, since the data is substantively identical.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

3.1.6. Summary statement of legal challenges for PA2

As the overview above has shown, PA2 can draw on the existing legal framework, notably the BRIS Directive and the BRIS Regulation for many challenges. None the less, a few unique distinguishing elements remain:

- Federation agreement: since PA2 builds on the existing legislative framework but is not identical to it, a contractual framework needs to be created that integrates data providers (the business registers) and data consumers (the public authorities using the push/pull services).
- Transparency: since PA2 doesn't operate on a legislative basis but on a contractual framework, measures will need to be taken to ensure that entities are informed of the fact that a public authority can (or may) be consuming information in relation to them.
- Revocability: entities must be able to revoke the push/pull right (e.g. by contacting the data consumer, or (less practically) the data provider). This may seem counterintuitive since largely the same information will be freely and publicly available anyway via the eJustice Portal BRIS service, but the latter operates on a legislative basis that ensures its lawfulness, whereas PA2 is a pilot that can operate under commercial terms, and may therefore otherwise be vulnerable to claims of unlawful commercial exploitation of business register information.
- Other requirements (e.g. in relation to security, interoperability, service quality etc.) can draw as far as possible from the BRIS Directive and BRIS Regulation; this will avoid divergences between PA2 piloting and the operational BRIS services.

Thus, PA2 can operate on the basis of a federated contractual framework in which the data providers agree to provide the specified evidence to identified data consumers, conditional on the awareness of the entities involved. The TOOP Business Register Federation could be created through accession agreements for data providers, and accession agreements for data consumers. The practical implementation details will however be examined in greater detail in the sections below.

Online Ship and Crew Certificates Pilot (PA3)

3.1.7. Summary description of PA3 and identification of PA3 specific legislation

PA3 relates to the exchange of evidence in a maritime context. Currently, ship and crew certificates are issued, maintained and exchanged in paper format, resulting in delays in delivery to the vessel and extra costs. The certificate data which is at the origin of the certificates exists in national Maritime Administrations (MA), which possess databases where certificate data are retained. PA3 aims to connect these databases and make the information available to the concerned parties.

PA3 thus relates to two types of certificates:

- The ship certificate: the vessel's flag state's MA and a recognized organisation issue the ship certificate (as is currently already the case on paper). Thereafter, the Port State Control (PSC), or any other interested party (e.g., Port Authority, Police and Border Guard Board, Charter Company), can view or check the certificate data through an online service. It is worth noting that the certificates describe the ship, not its current cargo.
- The crew certificate: the seafarer's national MA issues a crew certificate to each crew member, the ship flag state's MA checks the validity and authenticity of the crew certificate and the ship flag state's MA issues the endorsement of the certificate. Again, the PSC or any other interested party (e.g., Port Authority, Police and Border Guard Board, Charter Company etc.) can view and check the certificate data online.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

PA3 is legal underpinned through an extensive and complex international, EU level and national legal framework. At the international level, the International Maritime Organisation (IMO) has defined the principal rules:

- The 1974 SOLAS Convention (International Convention for the Safety of Life at Sea) [14] contains the basic rules in relation to the safety of merchant ships. It defines basic safety requirements, and a number of certificates are prescribed in the Convention, including inspection rights.
- The 1978 International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW Convention)[15] establishes the relevant international standards, including the substance and language of certificates, requirements for receiving them (depending on the function of the seafarer), procedures for issuance and endorsement by national administrations, expiration periods of certificates (5 years unless revoked earlier), and the legal obligation to keep any certificate required by the Convention "available in its original form on board the ship on which the holder is serving". It is worth noting that crew certificates include statements on the medical fitness of seafarers (section A-I/9 of the STCW Code[16]); this information is therefore not only personal data, but arguably also sensitive data since it contains data concerning health under EU law.
  Crucially also to PA3, it contains the obligation for each signatory to the STCW Convention" to *maintain a register or registers of all certificates and endorsements for masters, officers, and, as applicable, ratings which are issued, have expired or have been revalidated, suspended, cancelled or reported lost or destroyed and of dispensations issued. Each Party undertakes to make available information on the status of such certificates of competency, endorsements and dispensations to other Parties and companies which request verification of the authenticity and validity of certificates produced to them by seafarers seeking recognition of their certificates under regulation I/10 or employment on board ship. As of 1 January 2017, the information on the status of information required to be available in accordance with paragraph 15 of this regulation shall be made available, in the English language, through electronic means."* Thus, the STCW Convention provides a clear legal underpinning for PA3's objectives.
- The 1965 Convention on Facilitation of International Maritime Traffic (FAL Convention)[17], which regulates the number and type of declarations which can be required by public authorities in order to check compliance with maritime law. The FAL Convention contains "Standards" and "Recommended Practices" on formalities, documentary requirements and procedures which should be applied on arrival, stay and departure to the ship itself, and to its crew, passengers, baggage and cargo. Declarations covered include an IMO General Declaration and a Crew List Passenger List.

[14] http://www.imo.org/en/KnowledgeCentre/ReferencesAndArchives/HistoryofSOLAS/Pages/default.aspx

[15] http://www.imo.org/en/OurWork/humanelement/trainingcertification/pages/stcw-convention.aspx, http://www.imo.org/en/OurWork/HumanElement/TrainingCertification/Documents/33.pdf and http://www.imo.org/en/OurWork/HumanElement/TrainingCertification/Documents/34.pdf

[16] Defined at national level, but harmonised through the International Labour Office Guidelines on the medical examinations of seafarers; see http://www.ilo.org/wcmsp5/groups/public/@ed_dialogue/@sector/documents/meetingdocument/wcms_162824.pdf and https://www.samgongustofa.is/media/siglingar/ahafnir/WHO-Guidelines-on-Medical-Examinations-of-Seafarers.pdf.pdf

[17] http://www.imo.org/en/About/conventions/listofconventions/pages/convention-on-facilitation-of-international-maritime-traffic-(fal).aspx

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Other IMO Conventions such as the 2001 International Convention on the Control of Harmful Anti-Fouling Systems on Ships (AFS) and the 1973 International Convention for the Prevention of Pollution from Ships (MARPOL) can impact the use of certificates as well, but they do not have a direct impact on the execution of PA3.

From a European perspective, the main legal source is the Directive 2010/65/EU on reporting formalities for ships arriving in and/or departing from ports of the Member States[18], which simplifies and harmonises to the greatest extent possible the reporting formalities under maritime law, following the principles and templates of the FAL Convention. The Directive also provides further legal underpinning for SafeSeaNet, the Union maritime information exchange system developed and operated by the European Maritime Safety Agency (EMSA)[19] as a result of Directive 2002/59/EC establishing a Community vessel traffic monitoring and information system[20].

The Directive contains explicit rules on the electronic transmission of data, obliging Member States to "*accept the fulfilment of reporting formalities in electronic format and their transmission via a single window as soon as possible and in any case no later than 1 June 2015. This single window, linking SafeSeaNet, e-Customs and other electronic systems, shall be the place where, in accordance with this Directive, all information is reported once and made available to various competent authorities and the Member States*". Further interoperability and accessibility requirements are set out in Directive 2002/59/EC (which established SafeSeaNet) and Decision No 70/2008/EC a paperless environment for customs and trade.

The Directive 2002/59/EC furthermore obliges Member States to ensure that "*Information received in accordance with the reporting formalities provided in a legal act of the Union* (ed. such as the FAL documents) *is made available in their national SafeSeaNet systems and shall make relevant parts of such information available to other Member States via the SafeSeaNet system. [This information must be] accessible, upon request, to the relevant national authorities"*.

Collectively, the IMO Conventions and EU Directives provide broad support for the ambitions of PA3. The obligation for Member States to make information available via SafeSeaNet exists, in an electronic form, and a framework exists for establishing relevant standards. Admittedly, challenges exist as well: the IMO Conventions contain the obligation to keep certificates "available in its original form on board the ship on which the holder is serving"; this would suggest that electronic certificates are possible, but must be kept on board, and that pure online access may not be in line with the Conventions. A more constructive reading is also possible: the Convention requires that the certificates are kept on board the ship in their original form; it could be argued that if the original form is online access, then an implementation that ensures that online access on board is possible would arguable comply with the requirement as written. For certainty's sake, it may however be advisable to ensure that electronic documents can be stored in a fixed format such as PDF documents; that would at any rate comply with the requirement. More relevantly however, the certificates envisaged by PA3 do not fall within the stated scope of SafeSeaNet; PA3 thus extends the state of the art.

In order to achieve this objective, some revisions to current approaches will be required. In a paper environment, captains obtain paper certificates for their ship (as issued by the vessel's flag state's MA, via a recognized organisation) and for their crew (as issued by the seafarer's national MA). In practical terms, the captain is expected to keep these appropriately safe and to present them to competent authorities when required.

[18] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32010L0065

[19] http://www.emsa.europa.eu/ssn-main.html

[20] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002L0059

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Transitioning this to an electronic environment implies that captains must be able to electronically authenticate themselves towards the issuers of the certificates (MAs, including their recognized organisations) in order to request certificates in relation to their ship and crew. Similarly, competent authorities (PSC, Port Authority, Police and Border Guard Board, etc.) must be able to authenticate themselves in order to pull up relevant certificates, with the captain acting as the gatekeeper. The list of competent authorities is closely aligned with the scoping of SafeSeaNet[21], so this can be taken as a starting point.

Validation of the certificates may be more straightforward than might be expected: the IMO Conventions already require that crew certificates contain a unique identification code that can be used to validate whether the certificate is still valid. While this approach has clear flaws (notably in terms of access management and authorisation, since anyone holding the code can use it to validate certificates, irrespective of their competences), it is currently considered compliant and fit for purpose. At least from a legal perspective, it is therefore not a priority for improvement.

The main legal challenges for PA3 will be assessed by applying the legal assessment framework in the section below.

3.1.8. Application of the legal assessment framework to PA3

Having summarily described the specific legislation that applies to PA3, a more systematic assessment of legal challenges will be done using the legal assessment framework. In the table below, the requirements of the legal assessment framework will be applied to PA3, indicating whether there are any unique challenges or concerns (beyond those that would be required for any OOP use case).

[21] http://www.emsa.europa.eu/ssn-main/who-can-benefit-and-how.html

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Requirement of the legal assessment framework	Impacts which are specific to PA3 (if any)
Good administration requirements: • The OOP must be implemented in a way that ensures non-discrimination: evidence must be transferred on a neutral basis, without prejudicing any decisions that would be made by the receiving competent authority on the basis of the evidence. • The OOP must be implemented in a way that ensures transparency: the evidence to be transferred, the modalities of the transfer (specifically the duration of the accessibility of the evidence and the purposes of the exchange) and the categories of competent authorities involved must be clearly known to the persons concerned prior to the transfer. • If no evidence can be transferred, the competent authority must give reasons for this. • After the exchange, the receiving competent authority may only use the evidence for the purpose of the procedure for which the evidence was exchanged. as communicated to the persons benefiting from the OOP, excluding any use that is incompatible with the original purpose and any transfer to third parties (except where those third parties are required to achieve the communicated purposes). • The OOP must be implemented in a way that facilitates comprehension: without prejudice to the autonomy of the receiving competent authority, the person benefiting from the OOP should be able to receive information in relation to the evidence transfer process in his/her language of the Treaties.	Impacts: • None which are unique to PA3. Transparency towards crew members could be perceived as challenging, but should not present significant difficulties: the status quo is that a captain holds paper certificates that (s)he can show at will, and which can be verified by any third party using the unique identifier included on these certificates. From that perspective, PA3 only changes the modalities and increases security by building in logging/auditing controls. From a transparency point of view, PA3 improves upon the status quo, since post hoc controls are possible under PA3 (and not under the status quo).
Accountability requirements: • The OOP must be implemented in a way that ensures that all participants are aware of their obligations, and that the persons relying on the OOP have the right to restitution of any damages caused by noncompliance with these obligations insofar as this is possible under applicable law (i.e. taking into account possible exemptions of liability that may apply to the competent authorities under their national laws).	Impacts: • None which are unique to PA3.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Justice requirements: • The OOP must be implemented in a way that safeguards the right of every person to be heard, before any individual measure which would affect him or her adversely is taken on the basis of evidence exchanged via the OOP. • The OOP must therefore be implemented in a way that provides appropriate contact mechanisms for persons relying on the OOP towards all competent authorities involved as providers or as recipients of the evidence.	Impacts: • None which are unique to PA3.

Privacy, data protection and confidentiality requirements:
• The evidence exchanged via the OOP may only be processed in accordance with applicable data protection law when it contains any personal data, notably the DPD, or as of 25 May 2018, the GDPR. This includes the principles of:
  ○ lawfulness, fairness and transparency;
  ○ purpose limitation;
  ○ data minimisation;
  ○ accuracy;
  ○ storage limitation;
  ○ integrity and confidentiality;
  ○ accountability.
• When the evidence exchanged via the OOP does not contain any personal data, the competent authorities must still ensure that appropriate measures are taken to ensure an appropriate level of confidentiality of the evidence exchanged. When there is a legitimate confidentiality concern, the same principles as under data protection law can be applied.
	Impacts:
	• Given the scoping of crew certificates, data protection law will need to be complied with. In practice however, the envisaged data processing has a clear legal basis in the IMO Conventions, EU Directives and national laws implementing these. Processing is thus not based on consent of the crew member, but on legal necessity. Furthermore, with respect to each of the data protection principles, PA3 can improve on the status quo, since access to electronic certificates can and will be monitored (unlike for paper certificates). Access can and will be restricted to competent authorities (again unlike for paper certificates), with the captain's intervention acting as an additional safeguard. Thus, PA3 is a significant improvement upon the status quo from a data protection compliance perspective. It should also be highlighted that PA3 implies the processing of data concerning health, since the crew certificates also pertain to medical fitness. This is again justified on the basis of a legal necessity (the IMO Conventions requiring the exchange of this information). None the less, the processing of data concerning health is a further supporting element of PA3, since it is undeniably more secure and privacy oriented than the status quo.

Equality and solidarity requirements: • The OOP must be implemented in a way that ensures non-discrimination: evidence must be transferred on a neutral basis,	Impacts: • None which are unique to PA3.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

without prejudicing any decisions that would be made by the receiving competent authority on the basis of the evidence. • The OOP must be implemented in a way that ensures universal accessibility, including to persons with disabilities. Accessible support and communication mechanisms must be provided to ensure that such persons can receive comparable functionality as those persons benefiting from the OOP.	
Lawfulness and compliance requirements: • Evidence may only be transferred under the OOP between competent authorities if there is a legal basis for this, either the consent of the persons concerned or a separate legal basis such as a legal obligation; • Evidence may only be transferred under the OOP between competent authorities if it has been determined that any pre-existing legal requirements (including sector or context specific legal requirements) are satisfied, including national authorisation procedures, legal agreements on usage restrictions, assurances with respect to security, assurances or exclusions of liability, data or service quality arrangements, etc. During the course of the TOOP project, this will require a case by case assessment; after the entry into force of the SDGR this will likely be facilitated.	Impacts: • The legal basis for PA3 will be the IMO Conventions, EU Directives and national laws implementing these. As will be explained below, a federation agreement will need to be concluded between the public authorities accessing the certificates and the authorities issuing certificates; this will specify that the authorities will not access certificates via PA3 services without the captain's approval. If the scoping of the Directives and of SafeSeaNet would be expanded in the future, even this requirement (captain's approval) could be eliminated, allowing direct access to certificates between designated authorities. However, this ambition exceeds the scoping of PA3, since it is no longer an application of the OOP (defined in the proposed SDGR as requiring an explicit request of the user before a competent authority can request evidence directly from another competent authority - Article 12.4).
Control requirements: • Prior to initiating any evidence exchange, the competent authorities participating in the exchange must verify the link between the identity of the person benefiting from the OOP and the corresponding evidence. • Appropriate audit and logging measures must be implemented to ensure that any exchange of evidence organised under the OOP can verified by competent authorities in case of disputes (including the identification of the sending and receiving competent authorities, the time of the exchange, and the integrity/authenticity of the exchanged data itself).	Impacts: • For PA3 this is in practice resolved through the systematic intervention of the captain, authorising the transfer of certificates to the competent authorities. The captain acts in practical terms as a filter on the appropriateness of the information (as he already does when handing over paper certificates to authorities in a paper based process). The captain himself will however also need to receive an appropriate authentication mechanism to retrieve evidence. This can be built on national identification mechanisms. Compliance with the eIDAS Regulation is possible, but not mandatory for PA3. • Logging is necessary since the captain will in practice be able to access a broad range of certificates, which opens up an avenue for abuse. In practical terms,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

	captains are currently not linked to a specific vessel, so that they would be able to obtains certificates from other vessels than those they are piloting. They will therefore need to confirm via terms and conditions that they are acting as captains of the vessels for which they request certificates. Logging is in such situations absolutely crucial to be able to detect abuses (e.g. captains accessing and using certificates that they are not entitled to).
Value, validity and evidence requirements: • There must be an agreement between the competent authorities on the legal value and validity of the evidence, including specifically whether it can be considered authoritative (originating from and identical to information from an authoritative source or base register, i.e. any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity), or whether it can otherwise be assumed to be genuine.	Impacts: • This can in practice draw on the IMO Conventions and the EU Directives, which determine the value and validity of the certificates. It should be noted that the validity of crew certificates can already be validated by any third party through the unique identification numbers printed on each crew certificate.
Security requirements: • The competent authorities and any other participants in the evidence exchange mechanism must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: ○ the pseudonymisation and encryption of personal data; ○ the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; ○ the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; ○ a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	Impacts: • This can in practice draw on the IMO Conventions and the EU Directives, which define very high-level security requirements.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

• Incident response measures must be implemented to ensure that the exchange of compromised evidence is avoided and notified to recipients. Requirements under data protection law must at any rate be adhered to.	
Quality of data requirements: • A legal framework must exist that clarifies the obligations of the competent authorities in relation to the quality of the data, including any assurances of its accuracy, factual correctness, and timeliness of updates (which may take the form of legislation, SLAs, memoranda, or even nonbinding best efforts agreements; the requirement is that the understanding is clear). • A feedback mechanism must be in place that allows the persons involved to contact the competent authority at the source of the evidence to correct any inaccuracies.	Impacts: • This can in practice draw on the IMO Conventions and the EU Directives, since the data is substantively identical.
Quality of service requirements: • A legal framework must exist that clarifies the obligations of the competent authorities in relation to the availability and responsiveness of the services (which may take the form of legislation, SLAs, memoranda, or even nonbinding best efforts agreements; the requirement is that the understanding is clear). • An evaluation mechanism must be in place that allows noncompliance with this framework to be detected and addressed when necessary.	Impacts: • This can be based on the SafeSeaNet infrastructure.
Interoperability requirements: • Appropriate agreements must be in place with respect to the technical and semantic characteristics of the evidence to be exchanged between competent authorities, taking into account linguistic challenges and diversity of legal systems. Evidence should not be exchanged under the OOP if interoperability is not ensured.	Impacts: • This can in practice draw on the IMO Conventions and the EU Directives, since the data is substantively identical.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

3.1.9. Summary statement of legal challenges for PA3

As the overview above has shown, PA3 can draw on the existing legal framework, notably the IMO Conventions and EU Directives for many challenges. None the less, a few unique distinguishing elements remain:

- Federation agreement: since PA3 builds on the existing legislative framework but is not identical to it, a contractual framework needs to be created that integrates data providers (the Mas issuing certificates) and data consumers (the competent authorities that must be able to validate the certificates).
- Identification/authentication: the captains will in practice act as a filter to accessing the certificates. This implies that an identification/authentication solution is found, which must be integrated into the federation agreement. National solutions can differ, but mutual recognition must be ensured.
- Logging will be crucial to be able to detect and address abuses; this must be clearly communicated to captains.
- Given the obligation of the IMO Conventions to keep the original certificates on board, it should be possible to store certificates locally (e.g. as PDF documents). Signing and timestamping these can create significant added value, although this is not legally required.
- Other requirements (e.g. in relation to security, interoperability, service quality etc.) can draw as far as possible from the IMO Conventions and EU Directives; this will avoid divergences between PA3 piloting and the operational services of the SafeSeaNet infrastructure, which would likely be the long-term sustainability option for PA3 in Europe.

Thus, PA3 can operate on the basis of a federated contractual framework in which the data providers (Mas issuing certificates agree to provide the specified evidence to identified data consumers (competent authorities requiring access to the certificates - PSC, Port Authority, Police and Border Guard Board), conditional on the approval of the captain. The TOOP Maritime Data Federation could be created through accession agreements for data providers, and accession agreements for data consumers. In fact, this is identical to the model behind SafeSeaNet in the EU:

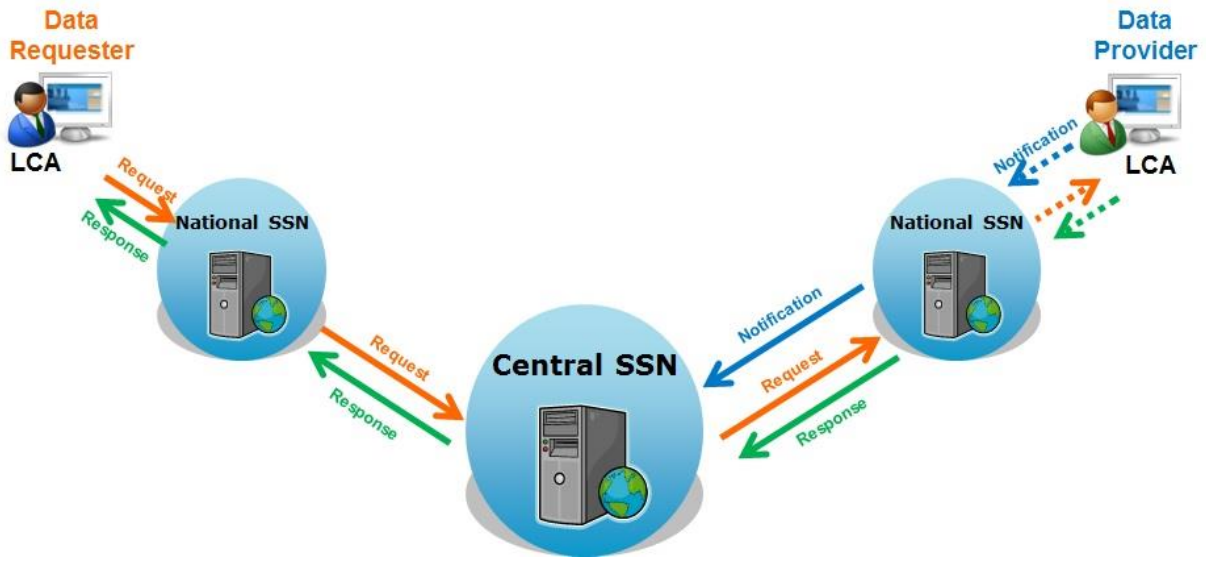

Figure 3: SafeSeaNet system - information exchange
(Source: http://www.emsa.europa.eu/ssn-main/ssn-how-it-works.html)

The practical implementation details will however be examined in greater detail in the sections below.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

4. The legal toolbox of TOOP

Introduction

The sections above have firstly defined a legal assessment framework that allows any OOP use case to be tested from a legal perspective (Chapter 2), and then identified legal challenges on the basis of this framework for each of the three TOOP pilot areas.

The objective of this deliverable is however not just to identify legal challenges, but also to find a way to resolve them. To do so, a legal toolbox is defined, containing the legal measures which are available within the context of the TOOP project.

Broadly, the following logical model can be proposed:

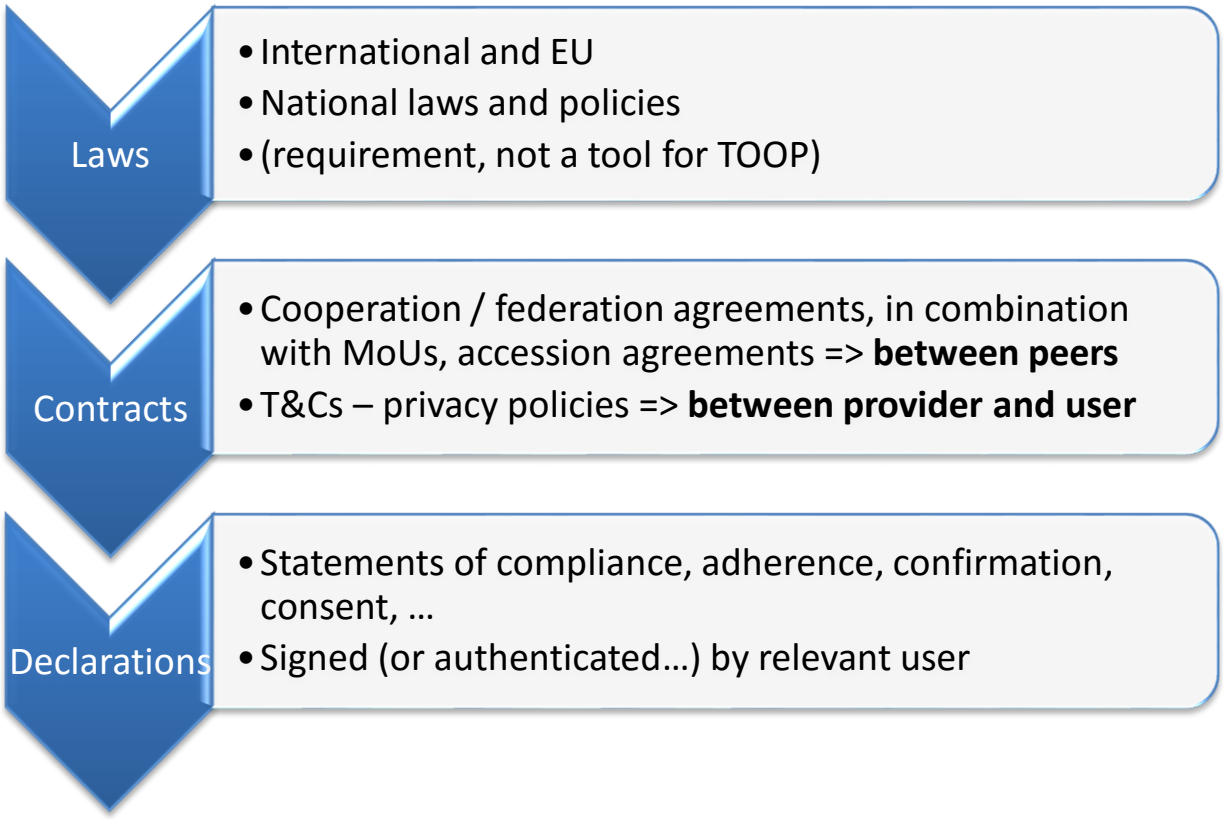

Figure 4: TOOP legal toolbox

In this figure, the first item ('Laws') refers to the legal context in which TOOP pilot areas operate, and which – for the purposes of the TOOP project – are considered static and immutable, in the sense that TOOP has no reliable way to change them in the course of the project. The laws that were used to define the legal assessment framework (notably the EU Charter of Fundamental Rights, Data Protection Directive (DPD) and General Data Protection Regulation (GDPR), eIDAS Regulation, PSI-II Directive, Services Directive and e-Commerce Directive) are a part of this context, as are the PA specific laws identified for each PA in Chapter 3. While these can evolve in the course of TOOP (and could theoretically even change in response to TOOP's findings), TOOP cannot count on these laws changing to match its needs. Put in a more pragmatic way: laws are not a tool that TOOP can use, but rather a requirement that it must work with.

The proposal for a Single Digital Gateway Regulation (SDGR) of course occupies a specific space in this framework: while it is currently still a proposal and therefore not a requirement as such, part of the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

objective of TOOP is precisely to learn lessons on how TOOP can be deployed at the EU level, making it significantly more likely that TOOP can shape the further evolution of the SDGR. For this reason too, the divergences between the legal assessment framework and the SDGR as commented in section 2.4 are not considered to be a weakness, but rather as a learning opportunity.

Considering that laws are outside TOOP's sphere of influence, there are two principal tools available to TOOP to resolve its legal challenges:

- **Contracts**, i.e. bilateral and multilateral agreements concluded between parties. This can include agreements between peers (such as federation agreements between competent authorities, agreeing to exchange certain evidences on the basis of predefined working conditions) and agreements which are imposed between providers and users (e.g. the terms and conditions presented to users, explaining the legal conditions for granting the permission to a competent authority for making evidence available to specific third parties).
- **Declarations**, i.e. unilateral statements made by one party towards another, from which the other party can derive certain rights or assurances. This includes statements of compliance with certain rules, confirmations that information contained in specific evidence is correct, or consent forms in which the user agrees that evidence can be presented to identified categories of recipients.

In the sections below, we will briefly examine the expected form and contents of these legal tools within TOOP.

Contracts in TOOP

The need for contracts in TOOP stems from the requirement to provide clear legal rules between data providers (the competent authorities that will make evidence available) and data consumers (the competent authorities that will receive evidence) on the one hand; and towards the users of the OOP (the persons whose evidence will be exchanged) on the other hand. Once the SDGR is in place, the need for contracts will likely be diminished or even eliminated entirely; but since this legal framework will not be in place for the duration of the TOOP project, a contractual framework is the most pragmatic solution.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

The general logical model for a TOOP federation looks as follows:

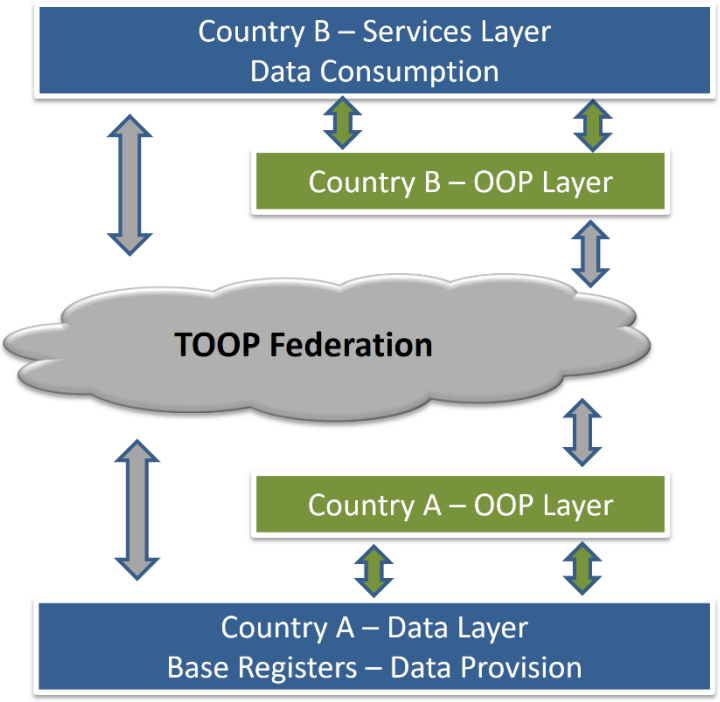

Figure 5: TOOP federation model
(Source: TOOP D2.1 (2017))

In this model, the TOOP federation contains the general rules, and data providers and consumers can accede to this federation. The latter implies that they conclude an accession agreement with the federation, detailing the terms under which they provide and/or consumer data. This model must be chosen since all data consumers must operate under the same rules, and all data providers must operate under the same rules; a mechanism in which legal assurances depend on the source or on the consumer would provide no legal certainty and therefore be unworkable in practice. Therefore, the core model is a static federation agreement with common rules for all participants, and accession agreements that essentially consist of a legal commitment to adhere to the rules of the federation, without negotiated variations between participants in the federation.

It is worth emphasizing that, while there can be only one federation agreement with common rules for the federation, it is possible that there are two types of accession agreements: one for consumers, and one for providers. This depends on the OOP use case: in situations where consumers and providers are the same entities (e.g. business registers) and have identical requirements and possibilities, a single accession agreement may be viable if all business registers are in precisely the same situation.

However, if the consumers are different from the providers (e.g. the business registers are data providers, and contracting authorities are data consumers), then separate agreements may be necessary if the interests of the participants are too diverse to capture all nuances in the federation agreement.

Ideally, the federation setup is very simple: a single federation agreement is established, and each participating country has precisely one participant, namely the entity that deploys the national OOP layer as shown in the model above. This is an ideally simple federation where the number of participants is precisely equal to the number of countries. Reality may not always be so simple, however, and in some PAs there may be many data sources or data consumers who are unwilling or

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

unable to unite behind one national contact point. This is not a deal breaker from the legal perspective (although it may be organisationally and politically less convenient): the legal model can scale to contain any number of data providers and consumers.

This scalability is also the reason why a federation/accession model was chosen, in which each participant concludes only one accession agreement with the federation. The alternative is a multilateral model in which each participant concludes an agreement with each other participant. This is not workable in practice, since the number of contracts becomes impracticably large with even a modest number of participants in a federation.

Thus, the model relies on federation and accession agreements. With respect to topics, the legal assessment framework provides the majority of the table of contents of legal topics that must be defined for each federation agreement:

- Preamble – the nature and goals of the TOOP federation
- General principles and accession to the federation
- Legal obligations of data consumers and data providers
    - Good administration
    - Accountability
    - Justice
    - Privacy, data protection and confidentiality
    - Equality and solidarity
    - Lawfulness and compliance
    - Control
    - Value, validity and evidence
    - Security
    - Quality of data
    - Quality of service
    - Interoperability
- Requirements for interactions with users
    - Terms and conditions towards end users
    - Data protection and privacy

This model allows each of the requirements identified in the assessments of Chapter 3 to be integrated into the federation agreements. The accession agreements, as noted, are relatively trivial, containing mainly the identification of the relevant party and their agreement to abide by the terms of the federation.

As a practical note, it is highly probable that, within the TOOP project, the federation and accession agreements will be established through memoranda of understanding (MoUs), rather than formal agreements. This avoids the need for formal signatures, since an MoU is a non-binding good faith only statement, which does not create new legal obligations and is not legally enforceable. While contracts are of course far preferable and will be attempted first, the implementation of federations through formal agreements can be burdensome, especially in pilot contexts, where partners are often reluctant to assume additional liabilities and responsibilities beyond their existing obligations under Grant Agreements, at least without having first tested the approach (as is, after all, the intention of a pilot project). Using MoUs rather than formal contracts would not be a unique approach to TOOP; large scale pilot projects such as STORK 2.0 have applied it as well, using it as a pragmatic stepping stone to the creation of a cleaner and definitive legal framework (which was the eIDAS Regulation for STORK 2.0, and might be the SDGR for TOOP). Therefore, if the conclusion of formal and binding contracts turns out to be impracticable, MoUs will be used as a backup solution.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Declarations in TOOP

Not every legal right needs to take the form of bilateral or multilateral contracts. It is also possible in practice that a declaration is used, i.e. a unilateral statement made by one party towards another, from which the other party can derive certain rights or assurances. The SDGR proposal also explicitly recognises this point when it requires in Article 12 that the technical platform "*shall enable the processing of requests for evidence to be exchanged*", and that the "*evidence made available by a competent authority shall be strictly limited to what has been requested and shall only be used by the receiving authority for the purpose of the procedure for which the evidence was exchanged*". Such requests can take the form of a unilateral declaration from the user agreeing to the exchange of evidence from a data provider to a data consumer.

Several forms of requests are conceivable and are a part of the TOOP toolbox:

- consent forms (requests in the sense of the SDGR) in which the user agrees that evidence can be presented by a competent authority to identified categories of recipients;
- statements of compliance with certain rules, e.g. confirming that the user is authorised to make a request on behalf of a specific entity or a declaration that evidence will only be used in a certain context;
- confirmations that information contained in specific evidence is correct. In principle, such confirmations should not be needed, since the entire purposes of the OOP is to ensure that authentic and trustworthy information is exchanged without a dependency on the user confirming their accuracy. However, involving the user can be beneficial in some cases, especially when the source itself might not be able to assert with complete certainty that the information was still accurate (e.g. because it is updated only annually, or because there may be a delay between update notifications and their integration into the source material); in these cases, a confirmation from the user can reduce some of the legal risk by ensuring that some validation can occur.

In practice, the various types of declarations mentioned above can be combined into a single document to reduce complexity.

From a legal perspective, the main challenge is ensuring the integrity and authenticity of the declarations, i.e. ensuring that they cannot be changed after the declaration is made (integrity) and that they can be uniquely linked to the person that made them (authenticity). These objectives can be easily reached by using the standardised eID and eSignature building blocks in the TOOP architecture (as explained in TOOP D2.1 (2017)), since their legal validity is supported by the eIDAS Regulation, ensuring recognition of the identities and signatures across the EU.

In practice, for the duration of TOOP, it is possible that alternatives will be used for pilot areas where no notified eIDs under eIDAS are currently being used, or where no signatures are used that appear on the EU trusted list as eIDAS requires. This can be the case within the EU (note e.g. that at the time of drafting of this deliverable no eIDs have completed the notification process as prescribed by eIDAS, so that mutual recognition is at any rate not legally ensured for eIDs), but also for international TOOP cases such as the maritime pilot, where the legal impact of eIDAS may not be sufficient to resolve all problems. Within the TOOP project, choosing alternative identification and signature solutions is perfectly viable, since acceptable identification/authentication tools can be defined in the federation agreement, with acceding parties accepting their use in practice.

None the less, the strong preference is of course to use the standardised eID and eSignature building blocks wherever possible, since this will greatly facilitate scalability and long-term sustainability.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

5. High-level initial definition of legal solution models for the three pilot areas and preliminary sustainability observations

Introduction – application of the legal tools in the PAs

Chapter 4 above has illustrated the tools which are available in order to organise legal compliance within the duration of the TOOP project. The present Chapter will examine specifically how they will be established and applied in each PA.

It should be noted however that, while the current draft of this deliverable provides the general model and structure that will be applied, including specific legal topics, the exact draft text of contracts and declarations has not yet been drafted. This is because, at the time of drafting of the present deliverable, motivational scenarios of each PA are still subject to discussion and evolution, meaning that definitive legal texts also cannot be provided. This is not problematic as such; the key objective of the present deliverable is to identify legal challenges and establish the general structure and approach of legal compliance measures. The implementation of contracts and declarations will continue after the submission of this deliverable, and will be maintained in the course of the TOOP project, so that contracts and declarations remain up-to-date with the evolutions of the TOOP project. This ensures that, rather than providing a static text in month 12 that may not match the realities, lessons learned can be integrated in the course of the project.

A second important point is the question of multiplicity of federations. The SDGR proposal envisages the creation of a technical system that will be used to support all of the OOP use cases within the scope of the proposal (as described in section 2.4 above). The architecture of the TOOP project applies the same model, which however splits the technical system into a common platform a 'TOOP Federation of Federations'), supplemented by a multitude of 'Domain Federations', which can be linked to the PAs:

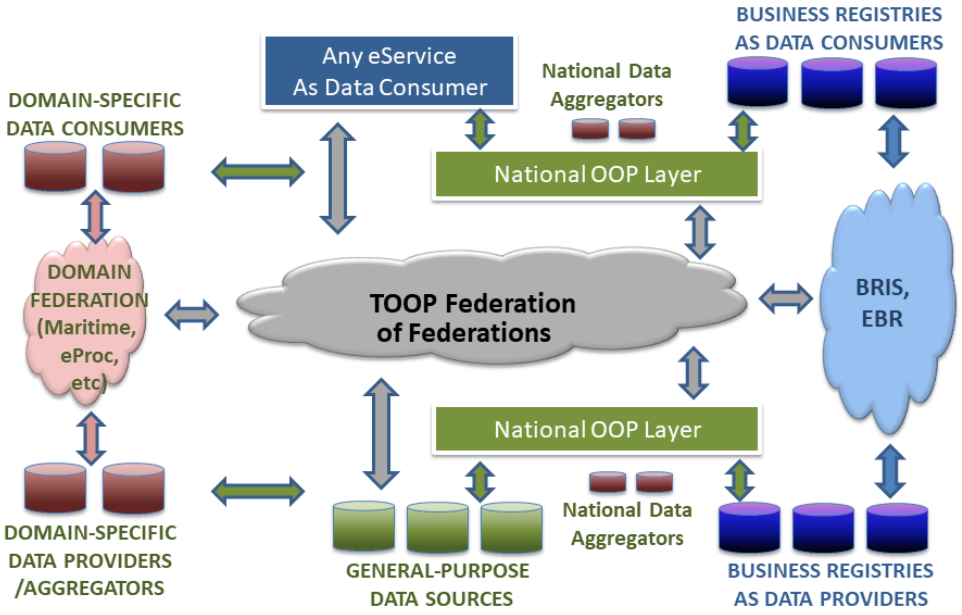

Figure 6: TOOP Federation of Federations
(Source: TOOP D2.1 (2017))

Thus, architecturally, TOOP operates as a single Federation of Federations, which harbours multiple data providers and data consumers, and can encompass Domain Federations. A crucial question then

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

is whether the legal setup can mirror this arrangement. In practice, mirroring this arrangement would imply a single Federation of Federation Agreement, to which data providers and consumers can accede (such as the business registers in the graph above), and which can branch out to other Domain Federations and other networks that act as a federation such as BRIS/EBR in the graph above. The latter would be governed by their own Domain Federation Agreements (or in the case of BRIS/EBR: their own legal framework), and conclude separate accession agreements with their domain specific data providers and data consumers (who would not necessarily be direct providers/consumers of the Federation of Federations).

This approach is viable using the general legal toolbox as described above. However, a key challenge will be to define exactly which elements can be aggregated to the Federation of Federations level, and which elements need to be defined within the Domain Federation. For this reason, initially the PAs will be set up as separate Domain Federation Agreements – which technically and architecturally will of course use the same components wherever possible – allowing the TOOP project to evaluate in the course of the project which elements of each Domain Federation are identical and therefore can be integrated in a Federation of Federations Agreement, removing them from the Domain Federation Agreement.

Initial definition of the legal solution model per PA

Based on the predefined legal toolbox of Chapter 4 and on the legal assessment per pilot area in Chapter 3, this section will provide a high level initial definition of the legal approach which is currently envisaged for each PA. As has been noted above, the current draft of this deliverable only provides the general model and structure that will be applied, while the exact draft text of contracts and declarations will be provided in the course of the project as the PA definitions mature.

5.1.1. Legal solution model for PA 1

As the earlier analysis of Chapter 3 showed, PA1 benefits from the fact that a partial legal basis for its motivational scenarios exists through the Public Procurement Directives, the Services Directive, the Professional Qualifications Directive and the BRIS Directive. However, none of these ensure the accessibility and availability of data in the business registers to third parties as envisaged by PA1.

The following key legal challenges were identified in Chapter 3:

- Scoping: it must be clearly delineated which competent authorities will be able to gain access to information in source registers. All motivational scenarios are predicated on the prior consent of the person concerned, so this can be built in as a safeguard.
- Legal recognition of the ESPD 'token' by third parties for motivational scenario 1, notably the competent authorities that would be providing evidence in response to the ESPD token. This is supported by the Public Procurement Directives, but requires operationalisation to ensure that competent authorities respond to the ESPD token.
- In motivational scenarios 2 and 3 (Licences and Permissions, Basic company data and Legal Person Mandates), there must similarly be a recognition by information providers of the legal request made by the end user to provide information from a business register (or other data source) directly to the authority envisaged (typically but not exclusively the Point of Single Contact as designated under the Services Directive).
- Ensuring the traceability and logging of any use of the token: breaches must be identifiable so that unlawful access can be detected and addressed.
- Revocability: the 'token' may not have an unlimited duration since that would cause confidentiality / privacy concerns. This can be done either by specifying a standardised

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

expiration date for the token, or by allowing explicit revocation. Standardised expiration dates would likely be more viable.

These needs could be satisfied by establishing a PA1 Federation Agreement that governs the basic functionality of PA1, including the limitations in terms of scoping, legal recognition, traceability and revocation. The PA1 Federation Agreement would furthermore also determine the process for creating and using an ESPD or other types of requests as a data access token (which would be a declaration in the sense of the legal toolbox of Chapter 4), as a result of which data providers would be willing to provide information on the basis of the token.

Data providers – principally business registers – and data consumers – principally contracting authorities and points of single contact – would accede to this federation through specific accession agreements. Note that, to reduce complexity, data consumers could also accede via prequalification systems, essentially implying that prequalification system operators would accede as data consumers, thus hiding some of the federated complexity behind this model.

5.1.2. Legal solution model for PA 2

The main existing legal framework underpinning the PA2 motivational scenarios are the BRIS Directive and the BRIS Regulation. None the less, a few unique distinguishing elements remain, as listed in Chapter 3:

- Since the BRIS Directive and Regulation do not address the functionality of the push/pull services directly, a contractual framework needs to be created that integrates data providers (the business registers) and data consumers (the public authorities using the push/pull services).
- Transparency: since PA2 doesn't operate on a legislative basis but on a contractual framework, measures will need to be taken to ensure that entities are informed of the fact that a public authority can (or may) be consuming information in relation to them.
- Revocability: entities must be able to revoke the push/pull right (e.g. by contacting the data consumer, or (less practically) the data provider). This may seem counterintuitive since largely the same information will be freely and publicly available anyway via the eJustice Portal BRIS service, but the latter operates on a legislative basis that ensures its lawfulness, whereas PA2 is a pilot that can operate under commercial terms, and may therefore otherwise be vulnerable to claims of unlawful commercial exploitation of business register information.
- Other requirements (e.g. in relation to security, interoperability, service quality etc.) can draw as far as possible from the BRIS Directive and BRIS Regulation; this will avoid divergences between PA2 piloting and the operational BRIS services.

These needs could be satisfied by establishing a PA2 Federation Agreement that governs the basic functionality of PA2, including the functionality, transparency requirements, revocability of push/pull rights, commercial terms (or at least the right for business registers to apply commercial terms for push/pull services; there is no strict legal need for these to be identical or reciprocal across the business registers), and the requirements from the BRIS Directive and (mainly) the BRIS Regulation, which can simply be incorporated by reference to reduce margin of discussion.

Data providers – principally business registers – and data consumers – essentially undefined and open at this stage, although this can evolve during the course of TOOP based on the needs and limitations of the data providers – would accede to this federation through specific accession agreements.

5.1.3. Legal solution model for PA 3

Finally, PA3 obtains much of its legal framework from IMO Conventions and EU Directives, as indicated in Chapter 3, with the following specificities that require a solution within TOOP:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

- Federation agreement: since PA3 builds on the existing legislative framework but is not identical to it, a contractual framework needs to be created that integrates data providers (the MAs issuing certificates) and data consumers (the competent authorities that must be able to validate the certificates).
- Identification/authentication: the captains of individual vessels will in practice act as a filter to accessing the certificates. This implies that an identification/authentication solution is used, which must be integrated into the federation agreement. National solutions can differ, but mutual recognition must be ensured.
- Logging will be crucial to be able to detect and address abuses; this must be clearly communicated to captains.
- Given the obligation of the IMO Conventions to keep the original certificates on board, it should be possible to store certificates locally (e.g. as PDF documents). Signing and timestamping these can create significant added value, although this is not legally required.
- Other requirements (e.g. in relation to security, interoperability, service quality etc.) can draw as far as possible from the IMO Conventions and EU Directives; this will avoid divergences between PA3 piloting and the operational services of the SafeSeaNet infrastructure, which would likely be the long-term sustainability option for PA3 in Europe.

These needs could be satisfied by establishing a PA3 Federation Agreement that governs the basic functionality of PA3, including the identification/authentication requirements, logging, availability and uptime of the certificate access/download services, and the requirements from the IMO Conventions and EU Directives, which can simply be incorporated by reference to reduce margin of discussion. Given that the functionality of PA3 is essentially international (extending beyond the geographic scope of the EU), preference should be given to references to the IMO Conventions where sufficient.

Data providers – principally MAs – and data consumers – competent authorities – would accede to this federation through specific accession agreements, that will affirm their willingness to accept the certificates made accessible under the terms of the PA3 Federation Agreement, at least for the TOOP piloting purposes.

Additionally, terms and conditions need to be drafted towards the captains, stressing their legal obligation (including under data protection law) to limited their access and use of the system to their legal tasks as defined under international and national law, and stressing that usage of the system is logged in order to be able to identify and address transgressions. As described in Chapter 3, this represents a significant advancement in terms of privacy and security compared to the current paper processes.

The importance of a clear legal basis

A key legal compliance question is of course whether there is a legal basis for the exchange of evidence within the TOOP pilots. This is addressed in the legal assessment framework by the 'Lawfulness and compliance' principle, which requires that the OOP must be implemented in a way that ensures that evidence is only transferred if there is an adequate legal basis for this, and in compliance with any applicable legal requirements.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

The pilots of the TOOP project to a large extent have a legal basis on which they can build:

- For PA1, the exchange of evidence in response to the ESPD token is supported by the Public Procurement Directives;
- For PA2, the exchange of evidence is supported by the BRIS Directive and the BRIS Regulation;
- For PA3, the exchange of evidence is supported by multiple IMO Conventions and EU Directives 2010/65/EU and 2002/59/EC, in addition to Decision No 70/2008/EC.

In each of these cases, participants in the pilots therefore have a legal framework that allows at least part of the pilots to be executed, and the contractual agreements that have been suggested in this deliverable merely serve to address the practicalities for which the participants have requested clarifications and guarantees through questionnaires and discussion meetings. This is of course also the only approach that a pilot project such as TOOP could take: since it is not capable of changing law, TOOP can only suggest support measures that build upon existing legal bases, not create them from scratch.

The mapping of the existing legal bases to the individual pilots is however not perfect; notably the push/pull functionality for business registers in PA2 is not addressed explicitly in the existing legal framework. This need not necessarily be a blocking factor if the business registers are willing and legally able to sign a contractual framework that permits the functionality to be created. In PA2, this may be viable due to the fact that at least some of the business registers are fully private or mixed status organisations (i.e. private undertakings acting under a public sector mandate), who could decide to execute the pilots as a part of their contractual freedom as private entities. For purely public sector bodies, it may not be possible to accept obligations that are not supported by law.

As the listing of the legal basis in the bullet points above shows, however, this assessment is highly context specific. The pilots in TOOP have at least a partial legal basis, with the possible exception of the push/pull functionality. This would not necessarily be the case for other OOP use cases. Indeed, the proposed SDGR explicitly covers a number of contexts for which no existing legal basis currently exists; as described in section 2.4 above, this relates to the following services:

- In Annex II of the proposed SDGR:
    - Requesting a birth certificate
    - Applying for a study grant from a public institution
    - Registering for social security benefits
    - Requesting recognition of diploma
    - Registering a change of address
    - Requesting/renewing ID card or passport
    - Registering a motor vehicle
    - Claiming pension and preretirement benefits from public or semi-public schemes
    - General registration of business activity, excluding procedures concerning the constitution of companies or firms within the meaning of the second paragraph of Article 54 TFEU
    - Registration of an employer (a natural person) with public or semi-public pension and insurance schemes
    - Registration of employees with public or semi-public pension and insurance schemes
    - Notification to the social security schemes of the end of contract with an employee
    - Payment of social contributions for employees
- Directive 2005/36/EC, on the recognition of professional qualifications
- Directive 2006/123/EC, i.e. the Services Directive
- Directives 2014/24/EU and 2014/25/EU, i.e. the Public Procurement Directives

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

None of these are addressed by TOOP, with the exception of PA1, which relates to a very specific component of the execution of the Public Procurement Directives, namely the use of the ESPD which already has a legal basis. For the other services in the SDGR, no legal basis indeed seems to exist today, and the SDGR would thus fill a clear gap.

Part of the objective of TOOP is to discover to what extent the OOP can be implemented in practice on the basis of existing laws supported by contractual agreements. Feedback through questionnaires from the participants thus far does not indicate that the lack of a legal basis is a blocking factor for the execution of the pilots; but this assessment may of course change as the pilot progresses and legal or policy barriers manifest themselves.

Preliminary sustainability recommendations

Sustainability questions will be examined in greater detail in TOOP D2.13 (the Sustainability Plan), based on the experiences in the pilots, in order to ensure the long-term usability of TOOP outputs. At the present stage of this legal deliverable, given that the envisaged contracts and declarations have not yet been drafted and that the pilots are not yet operational, meaningful sustainability recommendations are difficult to propose. None the less, a few preliminary recommendations and concerns can already be flagged.

Firstly, it goes without saying that the further development of the Single Digital Gateway Regulation will play a crucial role in ensuring the sustainability of TOOP outputs, in much the same way that the eIDAS Regulation has done for prior piloting experiences in relation to electronic identification, electronic signatures and other trust services.

On that point, it is worth reiterating the differences between the current TOOP approach and the current requirements of the SDGR. The scoping of the legal assessment framework of TOOP contains several details (e.g. in relation to quality of data and quality of service, or in relation to logging/audit/control mechanisms) which are not (yet) included in the SDGR. It will be worth assessing to what extent these will indeed prove to be valuable within TOOP, and can be integrated in the final SDGR and/or its implementing acts that the Commission is permitted to adopt under Article 12.7 of the SDGR to set out the specifications of the technical system.

Inversely, as noted in section 2.4, the SDGR contains a few principles that are not (yet) integrated into the legal assessment framework, notably:

- the requirement of an explicit request of the user before a competent authority can request evidence directly from another competent authority (Article 12.4);
- the obligation for competent authorities to make evidence available electronically provided that they issue evidence in electronic format within their own Member State (Article 12.5)
- a generic data minimisation principle requiring that “the evidence made available by a competent authority shall be strictly limited to what has been requested” (Article 12.6).

The reasons for the exclusion of these principles were outlined in section 2.4, and can be summarised as being driven by doubts on their viability and practical implications in practice for TOOP’s use cases.

These doubts are not necessarily relevant for the SDGR, which creates an autonomous legal basis for the exchange of evidence, and has a very clearly defined scope of application that does not correspond entirely with the three PAs of TOOP; notably PA3 (the maritime pilot) falls entirely outside the scope of the SDGR, as does the envisaged push/pull functionality. From a sustainability perspective, it will be worth evaluating in the course of the TOOP project whether and how these services can (or should) also be integrated within the SDGR’s scope of application.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

Finally, a key sustainability question will be to what extent all legal requirements relating to each of these diverging PAs can be homogenized and governed by the same rules. Within TOOP, this will be done through the PA specific federation agreements; when the three federation agreements are substantially identical on any given topic, this may be a good indicator that that topic is sufficiently generic that it can be applied across all OOP use cases, and therefore be suitable for inclusion in the SDGR as well (either in the primary text or in its implementing acts).

Thus, in summary, TOOP's sustainability largely depends on the possibility of inserting its findings into the SDGR and its implementing acts, in much the same way that earlier large-scale pilot projects provided findings that were incorporated into the eIDAS Regulation and its implementing act. On that point, TOOP will test specifically:

- to what extent the legal requirements of the SDGR can/should be broadened, considering the scoping of the legal assessment framework;
- to what extent the legal restrictions of the SDGR can/should be retained, based on the experiences that we will gain from the pilots;
- to what extent the scope of the SDGR is appropriate, given the PAs and their various motivational scenarios;
- to what extent the legal requirements of all PAs can be generalised into a central Federation of Federation (in terms of TOOP) or technical system (in terms of the SDGR).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Conclusion

Based on the analysis of this deliverable, it seems possible to execute pilots in each of the three pilot areas in compliance with current legislation. This is partially based on existing legislation, which in each case provides legal support for at least some of the requirements of the PAs. However, in the current absence of a generic legal framework for supporting the once-only principle (with the SDGR not yet having entered into force), the pilots need to be legally supported by an appropriate contractual framework, based notably on federation agreements which are pilot specific. This can be done and indeed will be done in the context of TOOP, but this approach is of course resource intensive (since contracts must be created on a case by case basis, and every participant must sign the agreement individually), somewhat unpredictable (since it depends on a willingness to sign), and prone to discussion (since any participant may ask that contracts are opened for negotiation).

Furthermore, there is one variable which a pilot project such as TOOP cannot control: if a participant feels that it would be contrary to its legal mandate to participate in the TOOP project (e.g. a public administration refuses to make its data available to its counterparts in other Member States because it has no explicit legal mandate to do so), there is no legal recourse to require it to participate. The SDGR would likely settle this issue, but its entry into application will likely take place after the conclusion of TOOP. The risk appears to be manageable within TOOP as all three pilot areas have a legal basis for at least part of their functionality, even in the absence of a general legal framework such as the SDGR.

Further assessment is needed as to how the contractual setup of TOOP can be integrated into the long-term vision of the SDGR. It is clear that the TOOP infrastructure could evolve into the 'technical infrastructure' envisaged by Article 12 of the SDGR, and therefore that some of the solutions envisaged by this deliverable could plausibly be integrated into the implementing acts contemplated by Article 12, thus ensuring that the lessons learned in TOOP – as described in the preliminary sustainability recommendations above - can be adopted in the implementation of the SDGR.

However, this will require some further maturing, both of the SDGR (the proposal as such is still relatively recent and may therefore still be refined) and of the solutions proposed in this report (as the pilots must still be implemented).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

References

TOOP Deliverables:

TOOP D2.1: Tepandi, J., Verhoosel, J.P.C., Zeginis, D., Wettergren, G., Dimitriou, J., Rotuna, C., Carabat, C., Albayrak, Ö., Yilmaz, E., Lampoltshammer, T., Täks, E., Prentza, A., Brandt, P., Kavassalis, P., Leontaridis, L., Streefkerk, J.W. (2017) Generic Federated OOP Architecture (1st version). Deliverable D2.1 of the TOOP project. Available at: http://toop.eu/sites/default/files/D21_Federated_OOP_Architecture.pdf

TOOP D2.6: Krimmer, R., Kalvet, T., Toots, M., Cepilovs, A. (2017) Position Paper on Definition of the "Once-Only" Principle and Situation in Europe. Deliverable D2.6 of the TOOP project. Available at: http://toop.eu/assets/custom/docs/TOOP_Position_Paper.pdf

TOOP D2.7: Kalvet, T., Toots, M., Krimmer, R. (2017). Drivers and barriers for OOP (1st version). Deliverable D2.7 of the TOOP project. Available at http://www.toop.eu/sites/default/files/D27_drivers_and_barriers.pdf

Other references

EU Charter of Fundamental Rights (2000/C 364/01); see http://www.europarl.europa.eu/charter/pdf/text_en.pdf, last visited on 12 July 2017

Proposal for a Regulation establishing a single digital gateway to provide information, procedures, assistance and problem solving services and amending Regulation (EU) No 1024/2012 (a Single Digital Gateway Regulation - SDGR), see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0256; last visited on 12 July 2017

Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:175:0001:0008:EN:PDF, last visited on 12 July 2017

Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market; see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0123, last visited on 12 July 2017

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML, last visited on 12 July 2017

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML; last visited on 12 July 2017

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); see http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679 last visited on 12 July 2017

Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation); see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG; last visited on 12 July 2017

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Contributors

Name	Surname	Organisation	Country
Graux	Hans	Time.lex	BE
Kustor	Peter	Bundesrechenzentrum Gmbh	AT
Koerner	Dörthe	Brønnøysundregistrene	NO

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Appendix I: Relevant national legislation in relation to the Once-Only principle

This overview will be expanded and maintained during the TOOP Project, and final findings will be integrated in D2.13 (the Sustainability Plan).

It is based on an overview created by the SCOOP4C project[22], but was expanded during the first stages of the TOOP project.

Country	Name, URL	Brief description of OOP case	Legal and/or policy grounds
Austria	FinanzOnline (FON), Austria, https://english.bmf.gv.at/e-government/portals/fon.html	FinanzOnline facilitates the access to the Austrian tax administration for citizens and businesses as well as for the public administration. Using FinanzOnline, Austrian citizens can, for instance, file their tax return electronically from home. The system contains already all salary data or social security contributions paid so that the citizen does not need to reenter these data. The tax account as well as all process steps can be traced online.	FinanzOnline Verordnung[23] is the legal basis for the whole online taxation procedure. It also regulates the data exchange between different public (and some private) entities and FinanzOnline for the provision of the related data along tax declarations for citizens and businesses.
Austria	Birth registration and family allowance (ALF – Antragslose Familienbeihilfe), https://english.bmf.gv.at/e-government/projects/alf.html	In the past, parents had to go to six different public agencies to carry out their duties and to be entitled to receive family allowance. Since May 1 2015, nine public services are integrated so that the parents only have to visit the Civil Registry Office and have to bring along (standard-case parents) no evidences except their personal identification (passport or personal ID card). In some cases, (lager local authorities), registry offices have even subsidiaries in hospitals so that the parents can do the whole procedure in the hospital. The personal data are stored in a couple of interacting registers, such as, central civil register (ZPR), central citizenship register (ZSR) and central residence register (ZMR). Through the service ”ALF“, it is possible to receive family allowance without having to fill an application upon the birth of a child. Automatic Family Allowances without Application (ALF) is a no-stop solution for	• The Austrian Act for family benefits 1967[24]. • Change of legal framework concerning the civil registration – allows cross-ministerial processing of personal data

[22] Specifically D1.2: Report on the state of play report of best practices; see https://scoop4c.eu/Materials

[23] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20004639

[24] https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2015_I_50/BGBLA_2015_I_50.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

		parents with which family allowances for new-born children are paid out automatically.	
Belgium	Unique data collection law http://www.ejustice.just.fgov.be/eli/wet/2014/05/05/2014203384/justel	The Belgian unique data collection law provides for a federal level legal recognition of authoritative data sources. It explicitly designates the national register number as the unique key identifying citizens, and mandates its use in information exchanges between public administrations. It provides legal recognition to service integrators, which are public sector organisations that serve to unlock data form authentic sources, and forbids participation public bodies to ask information from citizens if they can also obtain it via the service integrators.	Law of 5 May 2014 establishing the principle of unique data collection in the operation of services and instances providing public services, and simplifying and recognising the equivalence of paper and electronic forms http://www.ejustice.just.fgov.be/eli/wet/2014/05/05/2014203384/justel
Estonia	e-Notary, http://www.rik.ee/en/other-services/e-notary	The e-Notary system is an online environment, which helps notaries in their everyday work and allows electronic communication between notaries and the state. The system allows making queries to 16 different registries (for example the Marital Property Register, the Official Announcements, the Estonian Central Registry of Securities, the Register of Constructions, the Land Register, the Traffic Registry, the Land Cadastre, the Succession Register, the Population Register, the Registry of Recreational Craft, the Business Register). The system is owned by the Chamber of Notaries and the servers are administrated by the Centre of Registers and Information Systems.	• Notaries Act[25]. Riigikogu, RT I 2000, 104, 684. • Explanatory memorandum to the statute for keeping the e-notary information system[26]. • Notariaadimäärustik[27]. Riigikogu, RT I, 25.09.2015, 5. • Statutes of the electronic information system of notaries [28](e-notary). • Public Information Act[29]. Riigikogu, RT I 2000, 92, 597.

[25] https://www.riigiteataja.ee/en/eli/511032016002/consolide

[26] https://riha.eesti.ee/riha/main?araTopServiceId=application&araThreadServiceId=j3WXs51v&araTransactionId=override

[27] https://www.riigiteataja.ee/akt/13261784?leiaKehtiv

[28] https://riha.eesti.ee/riha/main?araTopServiceId=application&araThreadServiceId=a5fJ5rvz&araTransactionId=override

[29] https://www.riigiteataja.ee/en/eli/518012016001/consolide

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

			• The classification system[30]. Vabariigi Valitsus, RT I 2008, 4, 27. • The data exchange layer of information system[31]. Vabariigi Valitsus, RT I 27.09.2016, 4. • The administration system of state information system[32]. Vabariigi Valitsus, RT I 29.03.2016, 6.
Estonia	E-Tax, http://www.emta.ee/eng	Since 2002, the E-Tax system provides automated tax declaration forms. Each year, around 95 percent of tax declarations in Estonia are filed electronically. In 2015, one-click tax filing became available to Estonian citizens. Using a secure ID, a taxpayer logs onto the system, reviews their data in pre-filled forms, makes any necessary changes, and approves the document with a digital signature. The process typically takes three to five minutes.	• Taxation Act[33]. Riigikogu, RT I 2002, 26, 50. • "Tax registry"[34]. Establishment and Maintenance of the Register. Riigikogu, RT I, 26.05.2005, 11.
France	Programme 'Dites-le-nous une fois', http://simplification.modernisation.gouv.fr/wp-content/uploads/2016/10/DP-simplification_nouvel	As part of the programme "Dites-le-nous une fois", citizens do not have to hand in again certain documents to the tax authorities or any other authorities. The programme will start in the cities Paris, Lyon and Marseille, who have information about the family income and situation, as well as with information of the National Education, Higher Education and Research with data about scholarships in schools.	No legislative basis identified. See http://www.modernisation.gouv.fr/sites/default/files/fichiers-attaches/sgmap_plaquette_dlnuf.pdf for a summary of the policy plans.

[30] https://www.riigiteataja.ee/akt/12910889

[31] https://www.riigiteataja.ee/akt/127092016004

[32] https://www.riigiteataja.ee/akt/129032016006

[33] https://www.riigiteataja.ee/en/eli/502012017008/consolide

[34] https://www.riigiteataja.ee/akt/186654?leiaKehtiv

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

	les-mesures-particuliers-octobre2016.pdf	The programme also aims to mandate the exclusive use of the "siret number" as the unique identifier of companies that should facilitate information exchange between public administrations.	
Greece	TAXIS, http://www.gsis.gr/	TAXIS is the integrated information system of the Hellenic tax system. TAXISnet offers personalised information to citizens and businesses through its portal, as well as by sending automated emails. Since 2006, M-TAXIS service has been available. After the registration, citizens or businesses are informed for the tax that they have to pay by a SMS. Furthermore, they are informed about the deadlines of their payments. Recently, a set of web services based on TAXIS databases have been created and installed in the Interoperability Centre of the Ministry of Finance, as for example: • Confirmation of a person's details, • Tax registration data, • Certificate that a person or a company do not have any debts relevant to tax, • Certification for any debts of a person or a company to any public-sector organisation, • Vehicle owner details at a specific point of time. TAXIS promotes the Once-Only Principle by offering pre-filled forms. It acquires citizen data, such as salary details, from other information systems. Furthermore, it provides data to other governmental informational systems through web-services.	
Ireland	Data-Sharing and Governance Bill: Policy Proposals http://www.per.gov.ie/en/datasharing/ and http://www.per.gov.ie/wp-	In October 2013, the Department of Public Expenditure and Reform brought a 'Memorandum to Government', setting out a series of actions to improve data-sharing in the public service. Chief among these was the development of a Data-Sharing and Governance Bill. In July 2015, the Government approved the drafting of the Data-Sharing and Governance Bill 2015, along the lines of the General Scheme. The Scheme is based on granting permission to designated public bodies to share data from base registers (defined as "a database maintained by	The policy has been published, but no formal legislation has been adopted at this stage.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

	content/uploads/Appendix-I-Draft-General-Scheme.pdf	a public service body, subject to data quality and consistency checks and assurance procedures, which is designated by law as the authentic source of the data in question, and which is to be used by all public service bodies in the course of carrying out their functions"). Sharing may be done for any of the following purposes: (a) The prevention, identification, investigation and prosecution of offences; (b) To improve the provision of services by public service bodies; (c) To identify and correct erroneous data held by a public service body; (d) To collect debts owing to the State; (e) To audit the activities of a public service body; (f) To assess the effectiveness of a programme or policy. (g) Identifying, freezing, preserving or seizing the proceeds of criminal conduct	
UK	Tell Us Once, https://www.gov.uk/tell-us-once	Tell Us Once is a service which allows people to report a birth or death to most government organisations in one go. The Tell Us Once Database records details of the life event and the information recorded can include the data of birth or death, Names, National Insurance Number, Driving Licence and Passport details. Information is held for a maximum of 35 days then deleted.	Service provided by the Department for Work and Pensions (DWP) on behalf of Government. Details of the full Personal Information Charter for DWP can be foundon the Internet at https://www.gov.uk/government/organisations/department-for-workpensions/about/personal-information-charter.
UK	Making Tax digital (MTD), https://www.gov.uk/government/publications/making-tax-	The "Better use of information" foundation enables that individuals do not have to give HM Revenues and Customs (HMRD) information that it already has, or that it is able to get from elsewhere (e.g. from employers, banks, building societies and other government departments).	Finance Bill 2017[35], which is the vehicle for renewing annual taxes, delivering new tax proposals and maintaining administration of the tax system

[35] https://www.gov.uk/government/collections/finance-bill-2017

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

	digital/overview-of-making-tax-digital		
Netherlands	Base register system https://www.digitaleoverheid.nl/dossiers/basisregistraties/	The Netherlands has introduced a system in which base registers (*basisregistraties*) can get legal recognition, and thereafter are considered as the authoritative source of the data they contain. The legal basis is created via laws (one specific law per base register), but there are 12 central requirements (https://www.digitaleoverheid.nl/beleid/naar-een-gegevenslandschap/themas/twaalf-eisen-stelsel-van-basisregistraties/): • The register is governed by a law • Users have a reporting duty in case of errors or changes • Use is mandatory for the entire government • Liability is clear • Realisation and exploitation are at reasonable cost with a clear cost distribution model • The content and scope of the register is clear • There are clear arrangements and procedures between holders, users and data providers • Procedures for accessibility are clear • There are strict quality assurances • Participation of data users in governance is clearly regulated • The links between other registers are clearly established • Governance lies with a public body under the responsibility of a Minister. Eleven base registers currently exist (https://www.digitaleoverheid.nl/dossiers/basisregistraties/), covering persons, companies, land, income, addresses and buildings, etc.	Legislation is created on a per-register basis; see e.g. http://wetten.overheid.nl/BWBR0033715/2015-09-01 for the law on the person register.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Netherlands	StudieLink, http://www.studielink.nl	Studielink is the common registration and enrolment application for all non-private institutions of higher education in the Netherlands. Studielink arranges the exchange of information between the current or prospective student and the higher educational institution. Applicants can use Studielink to submit a digital enrolment application to an educational institution. Students can enter and check information which they can then access and use whenever they need it. This also applies for all bodies involved in the enrolment process, including universities of applied sciences, universities and DUO (Dienst Uitvoering Onderwijs - Education Executive Agency/Ministry of Education). Studielink is linked directly to authentic sources, such as the municipal personal records database (GBA), which includes personal data, and the IB-Groep's General Register for Student Numbers (including exam data). The result is a significant reduction in the paper-based bureaucracy for students and institutions. It also enables an increase in the quality of information sharing: since the information need only be entered and checked once, there is less chance of error than if several bodies enter and check the same information individually. As the staff members of the universities requested the implementation themselves, so they were eager to accept it.	• Higher Education Act[36] • Personal Data Protection Act [37]

[36] http://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=&p_isn=69514&p_country=NLD&p_count=2273&p_classification=09&p_classcount=29

[37] https://www.privacy.nl/uploads/guide_for_controller_ministry_justice.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460