DE4A
DIGITAL EUROPE FOR ALL

D7.4 Report on legal sustainability

Document Identification			
Status	Final	**Due Date**	31/03/2023
Version	1.0	**Submission Date**	03/04/2023

Related WP	WP7	**Document Reference**	D7.4
Related Deliverable(s)	WP4, WP7, WP8, WP9	**Dissemination Level (*)**	PU
Lead Participant	Timelex	**Lead Author**	Hans Graux (Time.lex)
Contributors	Pedro Demolder (Time.lex)	**Reviewers**	Gérard Soisson (CTIE) All partners

Keywords:

Legal, requirements, sustainability, compliance, SDGR, GDPR, eIDAS

Disclaimer for Deliverables with dissemination level PUBLIC
This document is issued within the frame and for the purpose of the DE4A project. This project has received funding from the European Union's Horizon2020 Framework Programme under Grant Agreement No. 870635 The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.
[The dissemination of this document reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains. This deliverable is subject to final acceptance by the European Commission.
This document and its content are the property of the DE4A Consortium. The content of all or parts of this document can be used and distributed provided that the DE4A project and the document are properly referenced.
Each DE4A Partner may use this document in conformity with the DE4A Consortium Grant Agreement provisions.

(*) Dissemination level: PU: Public, fully open, e.g. web; CO: Confidential, restricted under conditions set out in Model Grant Agreement; CI: Classified, Int = Internal Working Document, information as referred to in Commission Decision 2001/844/EC.

Document Information

List of Contributors	
Name	Partner
Hans Graux	Timelex
Pedro Demolder	Timelex

Document History			
Version	Date	Change editors	Changes
0.1	11/01/2023	Hans Graux (TLX)	Initial version of document – Table of contents
0.5	24/02/2023	Hans Graux, Pedro Demolder (TLX)	Initial analysis
0.8	07/03/2023	Hans Graux (TLX)	First contents and major outlines of all sections
0.9	13/03/2023	Hans Graux (TLX)	Finalisation for internal validation
0.98	03/04/2023	Hans Graux (TLX)	Integration of feedback from reviewers
0.99	03/04/2023	Julia Wells (ATOS)	Quality check, update of references
1.0	03/04/2023	Ana Piñuela Marcos (ATOS)	Final version for submission

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Hans Graux (Timelex)	03/04/2023
Quality manager	Julia Wells (ATOS)	03/04/2023
Project Coordinator	Ana Piñuela Marcos (ATOS)	03/04/2023

Table of Contents

List of Figures

List of Acronyms

Abbreviation / acronym	Description
ABB	Architecture Building Block
ADM	(TOGAF) Architecture Development Method
BB	Building Block
BRIS	Business Register Interconnection System
CEF	Connecting Europe Facility
DCAT	Data Catalogue Vocabulary
DE4A	Digital Europe for All (this project)
DLT	Distributed Ledger Technology
DSM	Digital Single Market
EESSI	Electronic Exchange of Social Security Information
EIF	European Interoperability Framework
EIRA	European Interoperability Reference Architecture
GDPR	General Data Protection Regulation
IR	Implementing Regulation of the SDGR
ISA2	Interoperability solutions for public administrations, businesses and citizens
LSP	Large Scale Pilot
N/A	Not Applicable
NRT	Near Real Time
OOP	Once Only Principle
OOTS	Once Only Technical System
OSI	Open Systems Interconnection model (OSI model)
SBB	Solution Building Block
SDG	Single Digital Gateway
SDGR	Single Digital Gateway Regulation (Regulation (EU) 2018/1724)
TBD	To Be Determined/Defined
TOOP	The Once Only Project, http://www.toop.eu/
VC	Verifiable Credentials

Executive Summary

This deliverable is the fourth and final formal output of WP7 (Legal and ethical compliance and consensus building) for the DE4A project. Its objective is to capture the possibilities, requirements and opportunities for the sustainability of the project from a legal perspective.

The report focuses on some of the realisations of the DE4A project that are more challenging to sustain from a legal perspective, principally because the project's general ambition is to explore and pilot optimal approaches to create effective once-only information exchanges, and to generally improve the efficiency and user friendliness of eGovernment in Europe, without necessarily focusing exclusively on the direct implementation of the EU legal framework (namely the SDGR). This has led to a number of useful innovations in the project, such as the multi-pattern evidence exchanges, the use of mobile wallets and verifiable credentials, and fine-grained powers validation – none of which have comprehensive and mature legal frameworks at the EU level at the present time.

In this report, these innovations are mapped against the sustainability mechanisms created by existing legal frameworks (including the SGDR, and eIDAS Regulation, and the Data Governance Act) and emerging legal frameworks (including the eIDAS 2 amendment proposal, the Data Act proposal, and the Interoperable Europe Act proposal).

The principal conclusions are that most of the project's innovations can be sustained to some extent, but also that there is a need for a broader legal framework at the EU level that can integrate and sustain these outcomes in a more holistic and flexible manner. Current legal frameworks take a piecemeal approach, each focusing on one specific topic, aspect or procedure of EU level eGovernment interactions. This approach has been beneficial in allowing the creation of useful building blocks and components.

However, it would be very useful, in the opinion of the project partners, to move towards a more agile and permanent legal framework for cross border eGovernment in the EU in general, that could more easily be extended to integrate existing building blocks, but also to cover new procedures, new legal requirements, new information exchange patterns, or new paradigms to determine the authenticity and reliability of government issued information. This would allow all outputs of the DE4A project to be integrated, sustained and expanded, without requiring ad hoc legal interventions that risk creating new layers of complexity, or creating real or perceived inconsistencies.

1 Introduction

1.1 Purpose of this document

The present document is the fourth and final deliverable in WP7 (Legal and ethical compliance and consensus building) for the DE4A project. The scope of WP7 is to ensure legal compliance of the project's execution with applicable legislation, notably the Single Digital Gateway Regulation (SDGR) and the General Data Protection Regulation (GDPR), but also other applicable rules, as well as ethics in general.

WP7 objectives include:

i) Continued assessment of existing and emerging legal requirements

ii) Assisting the translation of such legal requirements into technical, operational or infrastructural requirements

iii) Building consensus on best practices in compliance

iv) Providing inputs at the EU level on potential policy and legal follow-up actions, notably in the context of implementing acts of the SDGR.

One specific task of WP7 is Task 7.3 - Policy and legal sustainability recommendations. The goal of this task is to consider the longer term potential impacts and benefits of DE4A results beyond the project's duration. Under this task, DE4A should provide recommendations on how to ensure the sustainability of DE4A outputs from a legal perspective. To the extent that DE4A builds on the specific legal framework of the Single Digital Gateway Regulation (SDGR - [6]), this principally requires a consideration of the governance and sustainability mechanisms foreseen in the SDGR and its Implementing Regulation (IR - [16]), and an explanation of how DE4A outputs fit in.

However, there are a number of DE4A results which do not fit neatly or perfectly into the approach and provisions of the SDGR and its IR. The DE4A consortium aims to provide suggestions on how these can be sustained as well – either within the SDGR, within other EU level legislation (such as the eIDAS 2 proposal, the Data Governance Act, or the Data Act proposal), or via entirely new initiatives.

The goal of this report is to analyse to what extent DE4A results can already be sustained via current and planned regulatory frameworks at the EU level, and which other initiatives (if any) would be required or recommended in the future in order to fully reap the benefits of DE4A's experiences.

For the avoidance of doubt: this report is not intended to analyse or describe legal challenges or legal compliance activities in DE4A as a whole; these are instead captured in D7.3 - Final Report on legal and ethical recommendations and best practices [12].

1.2 Methodology for this report

The scope of the present report is inherently somewhat ambitious, since it aims to provide recommendations on future sustainability needs and on policy expectations in relation to eGovernment at the EU level. Opinions on this topic can reasonably differ between the project partners, since they somewhat depend on personal opinions as to what purposes and interests should be served by eGovernment services, and to what extent these should be realised at the EU level (rather than being addressed purely by Member State actions).

In order to arrive to a reasonable consensus, this deliverable was developed based on a preliminary list of DE4A outputs which did not appear to be fully sustained yet by existing legal frameworks at the EU level, along with a description of potential sustainability options, as provided by the WP7 team.

These outputs and the sustainability challenges and options were thereafter presented and discussed in a legal sustainability workshop, on 12 January 2023, to which all project partners were invited to participate. Meeting minutes of this workshop are attached to this report as Annex I. On the basis of the discussions during that workshop, the topics and challenges were reworked, and the present report was drafted. It was made available for review and commenting to all project partners in March 2023, and finalised on the basis of the provided feedback. The report can thus be considered to be a reasonable summary of the expectations and preferences of the DE4A project partners with respect to sustainability from a legal perspective.

1.3 Structure of the document

Apart from this introductory chapter and the Annex, this document is divided into three main sections:

- **Chapter 2 – General outline of the existing framework** for sustainability from a legal perspective. This chapter describes the legal frameworks that are already available at the EU level, or which are presently being proposed or redrafted, which could be used to support sustainability. A summary is provided of the scope of each legal framework in relation to sustainability, along with a short appreciation with respect to its applicability and utility to DE4A.
- **Chapter 3 – Analysis of legal sustainability requirements** as identified in the course of DE4A. This chapter identifies the DE4A results which have been identified during the DE4A project as potentially challenging from a legal sustainability perspective – either because the DE4A project has created innovations that are not directly or comprehensively supported yet at the EU level, or because it is unclear to what extent current legal frameworks will be applied. Where possible, follow-up actions are proposed and summarised.
- **Chapter 4 – Conclusions**. This chapter outlines the main findings and recommendations with respect to legal sustainability, including both 'quick wins' – i.e. sustainability challenges that can be addressed under the existing legal framework – and more fundamental problems that require more extensive policy consideration, and possibly entirely new legal frameworks.
- **Annex– DE4A Legal Sustainability workshop –** Minutes of the DE4A legal sustainability workshop held on 12 January 2023.

2 General outline of the existing framework for sustainability from a legal perspective

Since the objective of this report is to present opportunities and challenges for sustainability from a legal perspective, it is important to start with a basic understanding of the possibilities that are already available under existing legal frameworks at the EU level. After all, in the simplest possible scenario, every DE4A result could be neatly supported by existing legal frameworks, so that no entirely new initiatives would be necessary.

With that in mind, this chapter looks at four EU level frameworks to support sustainability from a legal perspective:

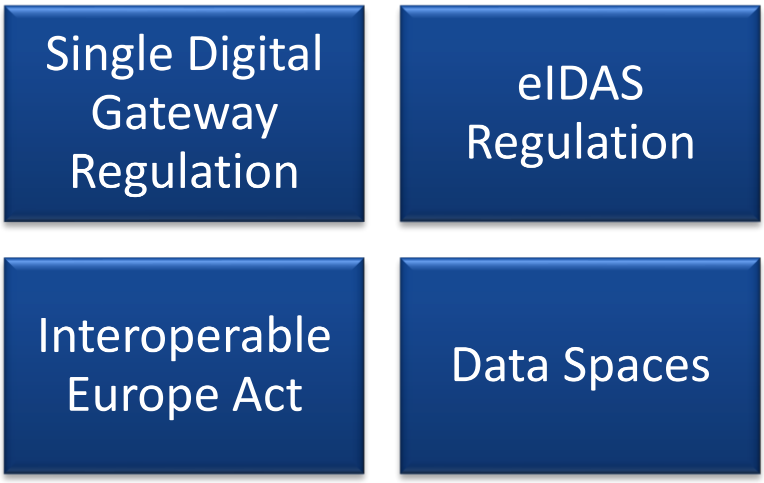


Figure 1: Four principal EU level legal frameworks for DE4A sustainability

Very briefly summarized:

- The **Single Digital Gateway Regulation** (and its Implementing Regulation) provides the central legal framework to support once-only information exchanges in EU level eGovernment services. It includes functional and architectural requirements for a specific technical system, and (most importantly for the purposes of this report) specific rules for governance and sustainability of the system.
- The **eIDAS Regulation** ([16]) (including the ongoing revision via the eIDAS 2 amendment proposal - [15]) provides the main rules in relation to electronic identification and certain trust services, including electronic signatures and registered electronic delivery services. The eIDAS 2 amendment would add specific rules in relation to European Digital Identity Wallets, electronic ledgers, and electronic attestation of attributes. Both the basic Regulation and its amendment contain specific governance and sustainability rules for these components and services.
- The proposal for an **Interoperable Europe Act** ([17]) was published in November 2022, and aims to strengthen cross-border interoperability and cooperation in the public sector at the EU level, specifically by defining shared governance mechanisms such as the creation of an Interoperable Europe Board to develop a common strategic agenda for cross-border interoperability, the support in operational implementing interoperability solutions, and progress monitoring; mandatory interoperability assessments to evaluate the impact of changes in IT systems related to cross-border interoperability in the EU; and the creation of an Interoperable Europe Portal to identify reusable and interoperable solutions and building blocks.

- The emerging **Data Spaces** policy field, as proposed by the European Data Strategy ([18]), and partially implemented via the **Data Governance Act** ([19])**,** to be further expanded and developed by the proposed **Data Act** ([20])**,** and a range of other initiatives. The central vision is to establish and support a range of sector specific "Common European data spaces", which bring together relevant data infrastructures and governance frameworks in order to facilitate data pooling and sharing. At least ten such Data Spaces are contemplated under the European Data Strategy, including a Common European data space for public administration.

In the sections below, we will briefly examine each of these frameworks, specifically with respect to their approach to governance and sustainability, and comment on their relevance and applicability to DE4A project results. A legal analysis of their substantive rules (i.e. excluding governance and sustainability) is outside the scope of this report.

As the short summary above indicates, the analysis considers both existing legislation that has already entered into force, and prospective legislation for which a proposal has been adopted by the Commission, but which has not yet undergone the full legislative process. In this way, the report can take into consideration expected (but not necessarily guaranteed) legislative evolutions in the near future, which can be quite relevant to DE4A as well.

2.1 Sustainability under the SDGR

2.1.1 Governance and sustainability rules in the framework

One of the objectives of the SDGR is to create a clear legal basis for the once-only principle at the cross-border level in the EU, and to support the establishment of a technical system for the automated exchange of evidence between competent authorities in different Member States. More specifically, article 14 of the SDGR requires that this system will support the exchange of evidence necessary for the completion of the procedures exhaustingly listed in annex II of the SDGR, as well as procedures governed by the Directive on the recognition of professional qualifications[1], the Directive on services in the internal market[2], the Directive on public procurement[3], and the Directive on procurement by entities operating in the water, energy, transport and postal services sectors[4].

Basic and high-level governance and sustainability rules are already defined in the SDGR itself, specifically in Chapter VII. The Commission and the Member States are responsible for the development, availability, maintenance, supervision, monitoring and security of their respective parts of the technical system. Organisationally, the SDGR establishes a network of national coordinators, designated by the Member States, to act as contact points and ensure that the national components of the technical system operate in accordance with the EU level specifications. A Gateway Coordination Group is also established, which includes one national coordinator from each Member State, under the chairmanship of a representative of the Commission.

The Coordination Group is tasked with supporting the implementation of the Regulation, and must, among other points:

(a) facilitate the exchange and regular updating of best practices;
(b) encourage the uptake of fully online procedures beyond those included in Annex II to the SDGR Regulation, and of online means of authentication, identification and signatures, in particular those provided for in the eIDAS Regulation;
(c) assist the Commission in developing common ICT solutions supporting the gateway;
(d) assist the Commission in monitoring compliance with the requirements of the technical system;
(e) provide opinions on procedures or measures to address efficiently any problems with the quality of the services raised by users or suggestions for its improvement;
(f) exchange best practices to enable the proper functioning of the common user interface of the technical system.

The governance mechanism is further developed via the SDGR’s Implementing Regulation, which principally develops functional and architectural requirements, but also dedicates a specific Section 6 of the IR to the governance of the technical system (referenced in the IR as the Once Only Technical System or ‘OOTS’). The Commission, in cooperation with the Gateway Coordination Group, must:

(a) oversee the establishment and launch of the OOTS;
(b) set priorities for further developments and improvements to the OOTS;
(c) determine an indicative schedule for the regular updates to, and maintenance and adaptation of, the technical design documents;
(d) recommend changes in the technical design documents;
(e) organise peer reviews to promote exchanges of experience and good practice between Member States on the application of this Regulation by Member States;
(f) approve or reject operational modalities submitted by any sub-groups established in accordance with the rules of procedure of the gateway coordination group, and, if needed, give specific guidance, and supervise their work.

Sub-groups established under the IR may draw up proposals of the operational modalities to be submitted to the gateway coordination group on standardisation of OOTS data models; evidence mapping; review, maintenance and interpretation of the technical design documents; operational governance, in particular operational arrangements and service level agreements; security, risk management and incident handling of the OOTS; and testing and deployment of the OOTS components, including interoperability between the national components.

2.1.2 Relevance to DE4A results

It goes without saying that the SGDR governance provisions are highly relevant to the sustainability of DE4A results, since to a large extent, DE4A pilots a potential blueprint for the SDGR’s technical system. As is explained in much more detail in D2.7 - Interoperability Architecture for Cross-border Procedures and Evidence Exchange in light of the Single Digital Gateway Regulation [28], the DE4A architecture description builds on the first version of the OOTS under the SDGR.

However, there are some divergences too: the SDGR focuses largely on the direct exchange of evidence between competent authorities in the context of SDGR procedures, and such exchanges principally happen only following the explicit request of the user, in combination with a prior preview option. DE4A on the other hand extends this approach to a multi-pattern architecture, which can raise sustainability and governance challenges, since the rules of the SDGR and IR would not allow the formalisation of an architectural logic that does not correspond to the choices made in the EU level legal framework. This issue will be explored in detail in the next chapter.

2.2 Sustainability under the eIDAS Regulation

2.2.1 Governance and sustainability rules in the framework

As is explained in more detail in D7.3 - Final Report on legal and ethical recommendations and best practices [12], the current eIDAS Regulation addresses three principal topics: electronic identification, trust services, and electronic documents. All three of these are relevant in the context of DE4A and the SDGR, and the SDGR and IR both reference it explicitly.

Very briefly summarised, with respect to electronic identification**,** the central objective of the eIDAS Regulation is to support the mutual recognition of certain electronic identities between Member States, specifically with a view to enabling access to e-government services. The eIDAS Regulation also comprises more than a purely legislative framework. Substantial development, implementation and development work has been organised at the EU and national level, resulting in the creation of the so-called eIDAS nodes. The eIDAS nodes can be understood as a standardised reference implementation software that Member States must deploy, operate and maintain, and which is capable of supporting cross border identification using notified eIDs.

With respect to trust services**,** the eIDAS Regulation creates a uniform legal framework for certain trust services, including electronic signatures, electronic seals, timestamps, and electronic registered delivery. Essentially, these comprise key building blocks of many digital transactions. The Regulation is integrated into OOP procedures via article 13 of the SDGR, which requires Member States to ensure that cross-border users are able to identify and authenticate themselves, sign or seal documents electronically, as provided for in the eIDAS Regulation, in all cases where this is also possible for non-cross border users.

The IR builds on this approach, since it also made support of the eDelivery Access points mandatory, thus including the electronic sealing and timestamping functionalities ingrained into this infrastructure. Equally importantly, the eIDAS nodes are referenced as a key tool for user authentication and identity matching functionality, thus building upon the electronic identification provisions of the eIDAS Regulation and on the requirements of article 13 of the SDGR. Under the IR, evidence requesters are required to rely on electronic identification means that have been issued under an electronic identification scheme that has been notified in accordance with the eIDAS Regulation.

In short, the eIDAS Regulation is closely integrated with the SDGR, meaning that the governance provisions of the eIDAS Regulation with respect to electronic identification and trust services are also particularly important. These are quite extensive, and arguably more explicitly regulated than under the SDGR:

- With respect to electronic identification, the eIDAS Regulation establishes an interoperability framework, comprising a reference to minimum technical requirements, a mapping of national assurance levels of notified electronic identification schemes, a reference to minimum technical requirements for interoperability, a reference to a minimum set of person identification data uniquely representing a natural or legal person, along with rules of procedure and arrangements for dispute resolution. This entire framework was adopted via two specific implementing regulations ([21]), which have remained in place since their adoption in 2015. Additionally, a separate regulation ([22]) establishes a cooperation network between the Member States, requiring the Member States to exchange information, experience and good practice as regards electronic identification schemes, in particular technical requirements related to interoperability and assurance levels; and tasked with the examination of relevant developments in the electronic identification sector.
- With respect to trust services, the eIDAS Regulation relies on the supervision of trust service providers via national supervisory bodies, who are bound to mutually assist each other in cross border matters, and who assess compliance with the eIDAS Regulation based on a series of standards that are referenced by EU level implementing regulations ([23]). These govern both the service providers themselves, the supervisory bodies, and certain products used in the provision of trust services.

The eIDAS Regulation is presently undergoing revision, and a proposal for an update to the eIDAS Regulation was published in June 2021 [15]. Among other topics, the proposal updates the minimal identity information to be made available under eIDAS notified schemes, clarifying that they must contain "a reference to a minimum set of person identification data necessary to uniquely and persistently represent a natural or legal person". The uniqueness and persistence of identifying data should further facilitate cross border identification.

Additionally, the Proposal provides a legal recognition of electronic attestations of attributes (including verifiable credentials), and provides both a definition, a non-discrimination principle and a legal recognition of electronic ledgers (defined as "a tamper proof electronic record of data, providing authenticity and integrity of the data it contains, accuracy of their date and time, and of their chronological ordering"). More significantly, it requires Member States to offer a European Digital Identity Wallet to their citizens. Such a Wallet should allow users to store identity data, credentials and attributes linked to their identity, and to:

a) provide them to relevant parties on request and to use them for authentication, online and offline, for a service; and

b) sign via qualified electronic signatures.

c) and allow for easy to use delegation

With respect to governance and sustainability, the Proposal largely respects the existing logic of the eIDAS Regulation. However, Wallets are treated in a somewhat hybrid manner, since they would be subject to prior notification procedures (like other electronic identification schemes under the eIDAS Regulation) but would also become subject to conformity assessment (like certain signature creation devices under the eIDAS Regulation). As such, they mix aspects of electronic identification and trust services from a governance perspective. The Commission would also be empowered to establish a list of standards for the certification of the European Digital Identity Wallets, and to establish technical and operational specifications and reference standards. While the Proposal is not yet definitively adopted, the first version of the European Digital Identity Wallet Architecture and Reference Framework was published in February 2023.

Thus, the eIDAS framework – including the eIDAS 2 amendment proposal – comprises a separate governance framework for key building blocks, including electronic identification, wallets, signatures, attribute attestations, and digital ledgers.

To be fully comprehensive, it may also be worth pointing out that, as a complement to the eIDAS Regulation and the eIDAS 2 amendment proposal, there is also the Pilot DLT Regulation ([25]). The Pilot DLT Regulation is, in a sense, a precursor to the eIDAS 2 proposal, since it already contains a legal framework for DLT services, albeit in a limited and sector specific manner. It creates a legal pilot regime for market infrastructures based on distributed ledger technology specifically for the financial sector. The Regulation starts from the observation that global financial markets were already experimenting with DLTs (namely in the context of crypto-assets) on a very large scale, and that the application of existing financial supervisory regimes to such assets is not a trivial matter, depending on the context and use cases.

To avoid regulatory gaps that create excessive risks to investor protection, market integrity, energy consumption and financial stability, the Regulation sets forth a dedicated regulatory framework, that establishes a system of permissions, conditions and exemptions for setting up and offering certain DLT market infrastructures.

Since it is a part of the EU's financial supervisory regime, the Regulation builds on the existing regime of competent (national) authorities that are tasked with supervisory duties under various existing EU level financial legislations, and on the European Securities and Markets Authority (ESMA) at the EU level to coordinate supervision and support the emergence of a common understanding of distributed ledger technology and DLT market infrastructure, to establishing a common supervisory culture and the convergence of supervisory practices, and to ensuring consistent approaches and convergence in supervisory outcomes.

The Pilot DLT Regulation is of course not directly applicable to the DE4A outcomes, which are not focused on financial services; but none the less it is useful as a demonstration of how an ad hoc instrument can be created to permit experimentation in a relatively unknown new field of technology.

2.2.2 Relevance to DE4A results

The eIDAS governance framework is highly relevant to DE4A, since DE4A relies on the eIDAS building blocks to a large extent. This includes the integration of support for Wallets, which have been included in DE4A's reference architecture, and its piloting activities in relation to verifiable credentials. Here too however, DE4A progresses the state of the art to some extent, since some of the piloted functionalities are not comprehensively covered in the existing framework (even assuming that the eIDAS 2 proposal would be adopted as currently written). This will be explored further in Chapter 3 below.

2.3 Sustainability with respect to interoperability

2.3.1 Governance and sustainability rules in the framework

The two policy topics discussed above – the SDGR and eIDAS respectively – each comprise their own governance and sustainability rules towards interoperability. Indeed, the governance mechanisms and decision making rules of these frameworks each stress the importance of interoperability in general, and contain a mechanism to address potential interoperability challenges within their scope of application.

None the less, the Commission also recently published its proposal for an Interoperable Europe Act ([17]), which should provide a horizontal framework to address interoperability challenges in the public sector at the EU level. The proposed Act builds on prior experiences with the non-regulatory European Interoperability Framework (EIF – [[27]]), under which Member States could build common eGovernment solutions, without however being in any way bound to contribute to them or rely on them in practice.

The proposed Act focuses on the creation of a more mature governance layer for eGovernment in Europe, without limiting itself to any specific topic (like electronic identification or once-only exchanges). It introduces a cooperation framework for public administrations across the EU that aims to foster the creation of shared digital solutions, such as open-source software, guidelines, checklists, frameworks, and IT tools. Specifically, it requires:

- A structured EU cooperation where public administrations, supported by public and private actors, come together in the framework of projects co-owned by Member States, as well as regions and cities.
- Mandatory assessments to evaluate the impact of changes in information technology (IT) systems on cross-border interoperability in the EU, if a public sector body wants to introduce or change a digital system that (potentially) uses/exchanges data from/to another Member State;
- The sharing and reuse of solutions, often open source, powered by an 'Interoperable Europe Portal' – a one-stop-shop for solutions and community cooperation.
- Innovation and support measures, including regulatory sandboxes for policy experimentation, GovTech projects to develop and scale up solutions for reuse, and training support.

A new Interoperable Europe Board would be established to support the interoperability cooperation framework, composed of representatives from the EU Member States, the Commission, the Committee of the Regions and the European Economic and Social Committee. Amongst others, the Board will have the mandate to agree on common reusable resources, support and innovation measures, and updates to the EIF. The Board would be supported by a community (the 'Interoperable Europe Community') that will enable the involvement of a broader set of stakeholders (including from the private sector), involved in the operational tasks linked to the implementation of the Regulation – an approach described in the proposal as multi-level governance. The Act would also require Member States to monitor and report on their level of interoperability on a regular basis.

The Act is not intended to replace existing governance mechanisms, e.g. in the context of the SDGR or eIDAS, which are generally more specific and prescriptive. Rather, the Act aims to facilitate the interoperable implementation of these frameworks, by setting up an ongoing structured cooperation around public sector cross-border interoperability.

2.3.2 Relevance to DE4A results

The Interoperable Europe Act can be particularly relevant to sustain DE4A results as well, in particular for any achievements that fall outside the direct scope of application of any of the other legal frameworks (e.g. with respect to multi-pattern exchanges or powers validation approaches, as will be discussed in Chapter 3 below). On these points, the Act could be used as a mechanism to identify relevant solutions and to promote their adoption across the EU. However, it is also worth noting that the Act fundamentally focuses on establishing governance mechanisms, not on establishing operational services or on regulating the legal value or legal impact of certain procedures. With that constraint in mind, the Act is relevant, but not a panacea that can be used to address any gaps in other legal frameworks.

2.4 Sustainability with respect to Data Spaces

2.4.1 Governance and sustainability rules in the framework

Finally, the last legal framework to be briefly discussed in this section is the emerging framework with respect to Data Spaces. As noted in the introduction, the concept of Data Spaces was first elaborated in the Data Strategy for Europe, which described their objective as "*bringing together relevant data infrastructures and governance frameworks in order to facilitate data pooling and sharing.*

[Data Spaces]:

(i) deploy data-sharing tools and services for the pooling, processing and sharing of data by an open number of organisations, as well as federate energy-efficient and trustworthy cloud capacities and related services;
(ii) include data governance structures, compatible with relevant EU legislation, which determine, in a transparent and fair way, the rights concerning access to and processing of the data;
(iii) improve the availability, quality and interoperability of data – both in domain-specific settings and across sectors."

The Strategy announced the creation of future data spaces in 10 strategic fields: health, agriculture, manufacturing, energy, mobility, financial, public administration, skills, the European Open Science Cloud and the crosscutting key priority of meeting the Green Deal objectives. In each instance, a data space would allow data from across the EU to be made available and exchanged in a trustworthy and secure manner, allowing businesses, public administrations and individuals in Europe to be in control of the data they generate, while knowing that they can trust the way in which it is used to boost innovation.

In terms of concrete legal frameworks, the Data Governance Act ([19]) sets a few common governance principles that should be respected by all data spaces, notably by designating a European Data Innovation Board. The Board is created as an expert group consisting of a broad range of representatives of relevant stakeholders (include competent authorities for data intermediation services, the European Data Protection Board, the European Data Protection Supervisor, ENISA, the Commission, and other representatives of relevant bodies in specific sectors as well as bodies with specific expertise). The Board is empowered to establish subgroups, including a subgroup for technical discussions on standardisation, portability and interoperability; and a subgroup for stakeholder involvement composed of relevant representatives from industry, research, academia, civil society, standardisation organisations, relevant common European data spaces.

In terms of its tasks, the Board should (among other topics) advise and assist the Commission on the prioritisation of cross-sector standards to be used and developed for data use and cross-sector data sharing between emerging common European data spaces, and propose guidelines for common

European data spaces, namely purpose- or sector-specific or cross-sectoral interoperable frameworks of common standards and practices to share or jointly process data. In this way, the Board could support the emergence of an EU Data Space for public administration, although it would require further legal action to actually create it.

Finally, within the proposal for a Data Act ([20]), Chapter VIII creates essential requirements to be complied with regarding interoperability for operators of data spaces (again however, without actually creating such a data space). Specifically, such operators would be required to satisfy the following interoperability requirements:

(a) the dataset content, use restrictions, licences, data collection methodology, data quality and uncertainty shall be sufficiently described to allow the recipient to find, access and use the data;

(b) the data structures, data formats, vocabularies, classification schemes, taxonomies and code lists shall be described in a publicly available and consistent manner;

(c) the technical means to access the data, such as application programming interfaces, and their terms of use and quality of service shall be sufficiently described to enable automatic access and transmission of data between parties, including continuously or in real-time in a machine-readable format;

(d) the means to enable the interoperability of smart contracts within their services and activities shall be provided.

The Commission is empowered to adopt delegated acts to further specify these essential requirements, and to adopt common specifications via implementing acts.

Collectively, there is a relatively mature body of governance rules to ensure the interoperability of data spaces.

2.4.2 Relevance to DE4A results

The Data Spaces framework is still at a relatively early stage of development. The European Data Innovation Board has a mandate that could be useful to support the emergence of a data space for public administration, and consequently to enable the integration of DE4A results into such a data space. However, it is worth repeating that the emphasis of the framework is currently solely on governance – not on operational services or legal value – and that no data space for public administration has been created yet at the present time. With that in mind, the framework is usable to further develop the DE4A outputs and to support awareness and even support among other Member States. However, it is not intended in its current form to mandate compliance with, or uptake of, DE4A results.

3 Analysis of legal sustainability requirements as identified in the course of DE4A

3.1 A general problem statement and the principal concern from the project partners

In the sections below, this report will examine a few specific instances where legal sustainability challenges have been encountered, and where it is not yet entirely clear how the project's achievements and advances beyond the state of the art can be sustained.

However, before looking at these more detailed issues, there is a central and cross cutting concern that was identified during the DE4A Legal Sustainability Workshop (as summarised in Annex I). Specifically, the DE4A project participants in that workshop raised the observation that cross border eGovernment was currently being addressed in a fragmented way at the EU level, and that coherence and consistency would be hard to achieve without a more comprehensive EU level legal framework that supports not only governance and interoperability discussions, but actually allows new eGovernment services and new interaction patterns to be created and sustained from an operational perspective.

By way of examples of the current fragmented approach at the EU level, the project can reference some of the prior legal achievements in the EU in relation to eGovernment as described above:

- The SDGR focuses on supporting and enabling specific user-initiated and -managed front office once-only exchanges, in specifically enumerated procedures (a closed list), with specific safeguards to protect confidentiality, privacy and quality;
- The eIDAS Regulation focuses on electronic identification in eGovernment services, and on trust services in general (i.e. without a specific focus on eGovernment services); trust services in the public sector fall within the scope of the eIDAS Regulation, but it contains no special rules for that context in particular. E.g. government eDelivery services can fall under the general legal framework for electronic registered delivery services, and government attestations can fall under the general non-discrimination rules for eDocuments, without specific rules to support their verifiability or legal authority beyond what would be possible in the private sector. Under the eIDAS 2 proposal, the proposed European Digital Identity Wallet is similarly a mixed instrument, with public and private interactions in scope – albeit with certain new provisions that support validation against official authoritative sources.
- The Interoperable Europe Act proposal takes a broader perspective, since it would create a legal framework to build and sustain governance rules for interoperability in general, but without focusing on operational services or legal implications;
- And the emerging Data Spaces framework could conceivably create a data space for public administrations, but so far only the rules for resolving interoperability problems have been defined in a general manner. No specific rules for an EU eGovernment Data Space have been proposed thus far.

Each of these components in isolation can work very effectively, and it is possible to rely on all of them to build specific eGovernment services on a case-by-case basis. However, there is a lack of an overarching legal framework that could cover a broad range of eGovernment services (not exhaustively enumerated, as is e.g. the case in the SDGR), that could create and run operational services (not just settle interoperability/governance discussions as is e.g. the case under the proposed Interoperable Europe Act), and that could create certainty on the legal value of cross-border eGovernment procedures (including the legal recognition of documents and resolving semantic issues in a targeted manner, unlike the more generic rules of the eIDAS Regulation).

One of the remits of DE4A is to pilot potential solutions that could satisfy the requirements of the SDGR; and one of the project findings is that it is indeed possible to implement the SDGR in a clear, reliable and effective manner. However, following the tightly scoped framework of the SDGR creates legal certainty at the expense of flexibility and functionality, since it has a clear focus on specifically listed procedures and specific exchange patterns that place the user – rather than the public interest – at the heart of any exchanges.

As D2.7 - Interoperability Architecture for Cross-border Procedures and Evidence Exchange highlighted [28], DE4A has created a flexible architecture that can be applied to a much broader range of public sector services, going beyond the principal focus of the SDGR. However, there is no clear and simple way to grant these additional services a clear legal value and to adopt them structurally in real-life scenarios at the EU level, despite their clear value to the public interest – and to the interests of users themselves, as will be explained below – except in the relatively narrow SDGR context. This could only be resolved by new legislative intervention that either fundamentally revises existing EU legislation, or creates a new horizontal legal framework.

The sections below describe several instances/manifestations of this broader problem. Solutions and potential paths for resolving them are not included here but will be discussed in Chapter 4.

3.2 Specific sustainability challenge 1 – Sustaining multi-pattern evidence exchanges

One of the principal innovations that DE4A has created, is the support for multi-pattern evidence exchanges. These are described in detail in D2.7 - Interoperability Architecture for Cross-border Procedures and Evidence Exchange, including an overview of how the patterns fit into the general DE4A architecture. The patterns include notably:

- The Intermediation Pattern
- The User-supported Intermediation Pattern
- The Lookup Pattern
- The Subscription and Notification Pattern
- The Push Pattern
- The Supported User-managed Access Pattern (or verifiable credentials pattern)

The SDGR does not explicitly support all of these patterns, since it focuses on user control as a general rule, via the mechanisms of explicit request and the preview option as referenced in Article 14. In essence, as a general rule exchanges via the SDGR's technical system may only occur after the explicit request of the user, and after the user has had the opportunity of previewing the evidences to be exchanged. This approach can protect the users against mistakes and abuses, since they are able to detect incorrect information before it is exchanged, and since governments in one Member State generally won't be able to access information held by an authority in another Member State without the active participation of the user.

The downside of this focus on user control is that it forces European governments to be reactive under SDGR procedures, rather than proactive: evidence is exchanged when this is asked by a user, rather than when this is beneficial in general. This is a very narrow concept of once-only exchanges, that arguably both under-represents:

- The **public interest**. The focus on user control does not account for the eventuality that a user behaves in bad faith, e.g. by providing evidences that they know will soon be corrected, or by allowing them to continue to reap the benefits that were granted on the basis of information that has become invalid after representing it (e.g. they have been authorised to provide a service that requires a clear criminal record, and know that they have been recently convicted. They actively decide not to make this information available to another public administration, since this allows them to retain their benefit unlawfully). The SDGR wouldn't allow such behaviour to be detected in many cases, since the user could refuse to request exchanges that would allow them to be detected. Exchanges would clearly be in the public interest, but the SDGR does not consider this as a sufficient reason to permit exchanges.

- The **private interest of vulnerable users**. While as a general rule, reliance on an explicit request seems to protect the user, this is certainly not always true. eGovernment exchanges can e.g. allow the automatic granting of benefits to vulnerable users (e.g. lower university enrolment fees for persons with less financial means). The SDGR approach would only grant such benefits to users that have the knowledge and ability to request them, but leaves digitally less capable persons in the cold – arguably the people that should benefit the most from efficient eGovernment exchanges.
- The **user's interest itself** (irrespective of whether a user is 'vulnerable' or not). A once-only approach that is only focused on front office user-initiated and user-managed online procedures makes the implementation of truly user centric automated, pro-active, back office procedures impossible. It is nevertheless obvious that it is very often far more user centric, efficient and once only to provide a service automatically and proactively without any request to the user to lose time and to invest effort to get this service.

Resolving this problem requires a rethinking of the safeguards behind once-only information exchanges at the EU level, or even of eGovernment in general: should Member States be allowed (or in some circumstances even required) to exchange certain information in the absence of a prior request, and without a preview option? Currently, the answer of the SDGR is largely no.

3.3 Specific sustainability challenge 2 – Citizen focus versus administration focus, including the role of mobile wallets and interrupted exchanges

The SDGR is fairly citizen centric where it grants the user control over procedures that they initiate and over any required evidence exchanges, and protects them against intrusions on their rights, interests or preferences by public administrations (which presents its own set of problems, as discussed above).

On other points however, it is relatively administration centric. With respect to evidence exchange patterns, it focuses on User-supported Intermediation by default: exchanges occur between competent authorities, with an intervention of the user towards the data provider to facilitate identity matching and verification of the evidence before it is exchanged. There is an interaction between the user and both the data provider and the data consumer, but the exchanges in principle happen between provider and consumer.

The reality can be a bit more complex in practice. Interrupted procedures, where the exchange of evidences cannot be completed immediately (i.e. within a specific authenticated and secured session) are possible – e.g. because one of the providers does not have the required evidence available immediately, or at least not in a digital form. In those instances, it should ideally be possible to interrupt / resume SDGR sessions, but this is not directly supported by the legal framework of the SDGR. The issue is architecturally not trivial, since it requires certain session data to be locally retained – and possibly actual evidences too – while a user is no longer 'in session'. This could create a possible user control gap in practice, depending on the implementation choices made, since data can be retained longer than could be required e.g. in the context of a preview space under the current SDGR. This issue is solvable through appropriate measures that e.g. continue to keep previewed evidences stored for an extended period of time in the secured preview space, but this requires both technical and legal safeguards.

Conceptually, it would also be possible to rely on European Digital Identity Wallets under the eIDAS 2 proposal as a workaround, since a Wallet would allow evidence to be stored decentrally, outside of the SDGR procedure and outside of the SDGR technical system, but this too has no direct legal support in the SDGR.

Moreover, the integration of Wallets into SDGR procedures for the specific purposes of sustaining interrupted procedures would represent an architectural and functional shift towards greater citizen centricity, which also however presents new legal and policy challenges. The SDGR was intended to facilitate specific evidence exchanges in specific enumerated procedures. Allowing Wallets to capture and store that evidence indefinitely allow a user to essentially use the SDGR as a generic process to obtain access to evidence, keeping a local copy, and use it as desired – including potentially sensitive information that would not normally be available to users without specific safeguards.

This problem can be solved by specific technical or architectural measures (e.g. by limiting the permitted storage time, or by encrypting it so that it can only be read by specific designated recipients, or by ensuring that it can only be shared if it is also re-validated against an authentic source at the time of sharing), but none of these are trivial to implement. This is a conceptual challenge when considering whether evidences should be managed centrally or decentralized.

3.4 Specific sustainability challenge 3 – Revocation of evidences, including in the context of verifiable credentials

It is interesting to observe that the SDGR does not consider or regulate the possibility of revocation of evidences issued under the SDGR – it only focuses on their issuance, exchange and use in the context of SDGR procedures. At least to some extent, this emphasis is likely due to the SDGR's focus on an exchange pattern where evidence should in principle be sent directly from one competent authority to another. The evidence is thus conceptually provided 'live' from the source, and should be immediately valid for the recipient (or at least as valid as the information held by the source).

The fact that the digital evidence may become invalid at a later stage (or that it is later discovered to always have been invalid) is 'out of scope' of the SDGR, in precisely the same way that it is 'out of scope' of traditional paper-based procedures: a paper attestation can only confirm (in the best of circumstances) that certain information was accurate at the time of issuing. It cannot possibly make any claims on what might have occurred afterwards; that issue is mainly resolved by risk management, i.e. by setting shorter or longer time periods after the issuing of a paper document during which it may be presented in a particular procedure ("*The extract must be issued during the last three months prior to submitting this form*").

In a digital environment however, it would be more easily feasible than in a paper environment to revoke evidences. This can e.g. be done by document specific electronic seals that can be revoked at the initiative of the signatory when sealed information has become inaccurate, or by allowing the relying party to assess the accuracy and validity of the evidence against authentic source data – i.e. by allowing "lookups" of the information contained in the digital evidence against an authentic source, where this exists.

This approach is partially in scope of the eIDAS 2 proposal, which discusses the use of authentic sources for some types of attribute assertions, and in the context of the Wallet. Specifically, eIDAS 2 would allow certain qualified attestations of attributes to be verified against authentic sources, either directly by the qualified trust service provider that issued them or via designated intermediaries recognised at national level. The proposal is very limited in scope, however, since it only focuses on a list of 10 explicitly enumerated categories of attributes (largely identity information for citizens); it is not conceived or suitable as a mechanism for universal revocability.

While imperfect, the eIDAS 2 proposal thus shows some attention to revocation; but that focus is missing from the SDGR. This is a defensible policy choice – the SDGR simply focuses on immediate exchanges, not on long term implications and benefits – but the lack of revocability also creates new risks that could be mitigated. This is particularly relevant in the context of verifiable credentials (VCs), since revocation of VCs is a standard part of their WC3 Data Model, which permits the creation of revocation registries, and thus a foreseeable functionality in the future.

None the less, there is currently no clear legal framework authorising the creation, use or reliance on revocation registries in an eGovernment context. Clearly, it is possible to create them already under the existing eIDAS rules, but no competent authority currently uses them or relies on them, and a competent authority in an SDGR process therefore also has no framework that would allow them to reject an evidence issued in the form of a VC when a revocation registry would show that it had in fact been revoked. This would require a clearer legal framework.

Moreover, it is not entirely clear – no significant debate has been held on this point – whether such revocation registries are necessary or beneficial in the European eGovernment context. Such registries would effectively create a second layer of registries: there are currently already authentic source databases in many Member States that could be used to verify whether information in a credential is still up to date. Adding a layer of revocation databases creates a new functionality, but one that is arguably redundant, depending on implementation choices: if a credential can be checked against its authoritative source, a revocation register has no additional benefit, especially if authentic sources can automatically and proactively revoke evidences in wallets that are no longer valid.

Simply applying the eIDAS 2 approach of verifying a VC against an authentic source in the SDGR context is not trivial either. The eIDAS 2 proposal however only governs a small subset of credentials that could be verified against an authentic source. Specially, it includes a minimum list of attributes in Annex VI, comprising address, age, gender, civil status, family composition, nationality, educational qualifications, titles and licenses; professional qualifications, titles and licenses; public permits and licenses; and financial and company data. *If* these attributes rely on authentic sources within the public sector, then qualified providers of electronic attestations of attributes should be able to verify their authenticity at the request of the user. Given the constraints – a minimum lists of attributes, the dependence on authentic sources, the prior request from the user, and the assistance of a qualified trust service provider – it is not a comprehensive solution within the context of the SDGR.

It is worth underlining however that some of the DE4A interaction patterns (notably the Lookup Pattern, the Subscription and Notification Pattern, and the Push Pattern) could facilitate verification of certain information contained in evidences after their issuance, and that they could even 'push' an invalidity message to a recipient where none had been requested, making active revocation an option in addition to passive verification. But, as noted above, these patterns are not directly supported by the SDGR.

3.5 Specific sustainability challenge 4 – Powers validation and representation rights

The representation of one person by another in any given process is a very important and very common legal problem, the most basic and common examples being a natural person's right to represent a legal entity (e.g. a director representing their company), or a parent's representation of their child.

Despite this importance in practice, representation is only very indirectly addressed by EU level legislation, notably in the eIDAS Regulation. The Regulation does contain basic rules for representing legal entities, and a minimal data set to identify such legal entities, but there is no framework for determining the exact competences of a representative of a legal entity. This is also a complex matter, of course, since representation rights are not harmonised at the EU level, and can thus depend not only on the Member State, but also on the type of legal entity, the type of representative, and the procedures involved.

As a practical result, representation of legal entities under the current eIDAS Regulation is only supported to a limited extent by the Member States – only two Member States have notified legal person eID schemes to the Commission. This means that powers validation for legal entities currently relies mainly on so-called 'full powers'-representation – i.e. where available, the eIDAS mechanisms can indicate whether a person has the broadest possible powers of representation for a specific legal entity (i.e. the rights that would normally be conferred to the general manager or CEO of a company), without supporting more details or more granularity.

The SEMPER extensions to the eIDAS nodes were created to address this problem. Specifically, the SEMPER project (Cross-border **SEM**antic Intero**PER**ability of Powers and Mandates) defined the semantic definitions of mandate attributes and enhanced the eIDAS Interoperability Framework with appropriate elements on protocol level and integration modules for connecting national mandate management infrastructures. DE4A has piloted this approach by amending the eIDAS node implementations of certain Member States to allow so-called "fine-grained powers validation".

While this provides a functioning solution in many contexts, it is important to note that the approach is not entirely comprehensive, and requires further take-up and support to improve interoperability, and to grant the extensions some legal authority. This issue may be taken up via the eIDAS 2 proposal – although it is worth noting that the proposal focuses only on the verification of officially registered mandates to represent legal entities (mainly companies). Other types of mandates – such as contractual mandates – are not in scope, and there is also currently no framework at the EU level to establish the legal power of one natural person to represent another (e.g. a parent's right to represent their children). This is a highly complex issue, that will however require resolution at some point.

4 Conclusions

4.1 Principal observations and lessons learned

DE4A has successfully created and piloted several components and exchange patterns that can be used in the implementation of the SDGR. More importantly however, the results of DE4A go beyond the SDGR – as was intended from the onset – and show a number of architectural and functional possibilities that seem highly desirable from a policy perspective, looking at e.g. the Tallinn Declaration [33] and the general objective of providing effective, efficient, reliable, automated and proactive government services to EU citizens. These do not always have a clear legal framework, as was described above in relation to multi-pattern exchanges, interrupted procedures, revocation of evidences, the role of verifiable credentials, and the need for clearer and unambiguous rules on representation powers and mandates.

The sections below will present a few avenues to facilitate sustainability on these points under the existing and emerging legal frameworks. However, the horizontal observation from the project members is that it would be useful to establish a broader horizontal eGovernment framework at the EU level that more easily allows cross border eGovernment procedures to be established, that allows any EU level eGovernment enabling infrastructure to be set up and maintained permanently and provides a clear legal value to these procedures and the exchanged information, beyond the current focus on governance and interoperability.

In effect, within DE4A, there is an interest to approach eGovernment by creating a legal "meta-framework" for cross-border eGovernment services in the EU that goes beyond mere interoperability, and beyond current notions of once-only services as encompassed in the SDGR. The goal should be to establish a long term framework that can flexibly address all eGovernment needs (including new procedures and new patterns), integrating existing building blocks, but without the need for ad hoc new legislative interventions in each instance.

4.2 Recommendations on sustainability actions outside of DE4A

4.2.1 Quick wins

For some of the specific sustainability challenges discussed above, partial quick wins are available that can resolve the most pressing problems:

- Within the Gateway Coordination Group under the SDGR, the existing governance mechanisms can be used to discuss to what extent multi-pattern approaches can be supported under the current SDGR, and to what extent interrupted procedures could be addressed. Comprehensive support of *all* multi-pattern approaches would not be possible, but there is arguably some margin for flexibility by maximally using:
    - The right of the user to request specific exchanges, e.g. by allowing this request to remain valid for a longer period of time (rather than just for the duration of a live session);
    - The exceptions to the requirements for an explicit request or for the preview option.

  This approach is however not ideal for all use cases. It can be perfectly appropriate for information that would at any rate be publicly available, since there is no notable confidentiality or data protection challenge in those cases, and the SDGR is, in such cases, just used for its infrastructural model. In other cases however, where information is more sensitive, using the exceptions can be impossible, or lower the level of protection afforded by the requirements of the SDGR,. At the very minimum, discussions could be organised to what extent and under which circumstances this can be considered both beneficial and legally compliant.

- Similarly, the Gateway Coordination Group could consider under which circumstances evidences could be issued as VCs, building on the framework for (qualified) electronic attestations of attributes under the eIDAS 2 proposal. Part of this workstream could leverage the revocation possibilities of VCs that are missing from other types of digital evidences, or (perhaps more plausibly) expand on the ways that verifiable credentials can be validated against authentic sources as is already foreseen under the eIDAS 2 proposal at a fairly tightly circumscribed scale (minimal list of attributes, prior user request needed, and mandatory intervention of qualified trust service providers).
- Within the ongoing eIDAS revision, further focus would be needed to integrate, formalise and maintain/expand the fine-grained powers validation of company representation rights, as piloted both under SEMPER and DE4A.

4.2.2 Fundamental issues

Beyond these quick wins, there is a set of more complex and fundamental issues that do not seem to fit cleanly into the existing legal framework. These would require EU level policy discussion to determine whether there is a consensus on the need to resolve these. They include notably:

- The establishment of a legal framework that allows certain exchanges of information in the public interest, or for the benefit of citizens or business, even in the absence of a prior request (i.e. to enable proactive government services, and to prevent fraud / other abuses). This would require a definition of such exchange mechanisms (e.g. based on the Lookup Pattern, the Subscription and Notification Pattern, and the Push Pattern piloted in DE4A, and including ways to define new exchange patterns), the circumstances in which such exchanges can occur, the identification of competent authorities that could participate in such exchanges, and likely a description of procedures in which they could be applied. Safeguards to protect citizens against risks and abuses could be integrated directly into this framework. It could be considered to integrate this into the discussions around a Data Space for public administration.
- The establishment of a legal framework that allows new eGovernment services to be addressed flexibly at the EU level, without having to create a new legislative framework for each specific initiative. Essentially, this would help to overcome the 'closed list' constraint of the SDGR, which leads to complex discussions on what exactly falls within its scope (e.g. the discussions on whether registration of an address in one Member State would necessitate deregistration in another Member State – this is currently a matter of national law, with unclear obligations and implications at the EU level[1]). This could also include a more generic framework for determining the integrity, authenticity, value and semantics of government issued documents, combining the logic of the infrastructural model of the SDGR with the newer provisions relating to qualified attribute attestations of eIDAS 2. Again, this could be made a part of a possible Data Space for public administration.
- The establishment of a more mature framework for representation in general, not only in relation to companies (which can be partially addressed in the eIDAS context), but also more broadly. This may be conceptually very difficult, since notions of representation (e.g. of parents and guardians towards minors or towards persons with diminished legal capacities) will undoubtedly vary across the Member States. It is not clear if/how these can be mapped and implemented in eGovernment services across the EU without harmonisation of these notions (much in the same way as a perfect

[1] The SDGR notes that such a procedure "*might consist of two separate procedures, one in the Member State of origin to request deregistration from the old address, and the other in the Member State of destination to request registration at the new address. Both procedures should be covered by this Regulation*" – however, this approaches the issue as two independent procedures, which should be interlinkable instead.

mapping of competences of company representatives is exceedingly difficult without harmonising company law to some extent).

- Moreover, a debate would be needed on the interactions between more user centric and more decentralised approaches (e.g. based on Wallets, VCs, and SSI), versus the more centralised approach of the SDGR and eIDAS 1 Regulation (eIDAS nodes, competent authorities, and specific designated infrastructure). As DE4A shows, it is possible to combine and interconnect those. There is however a significant functional overlap that causes doubts and inefficiencies (e.g. what is the role of a preview requirement when evidences are stored in a Wallet? How does an explicit request work for evidences in a Wallet? How do you reconcile the concept of once-only exchanges between competent authorities with a model where the user manages their own data). These need to be addressed consistently across the EU.

It seems clear that these fundamental issues require a broader legislative intervention at the EU level, rather than the mere streamlining of the application and interpretation of existing laws, and the finalisation of currently proposed laws. Possibly, the ongoing Data Spaces discussions are a fruitful avenue for exploring these topics further. A track exists to address the synergies between eIDAS 2 and the SDGR OOTS, via the so-called "OOTS and EUDI Wallet Synergies and Interoperability Contact Group", which has the formal remit to look for such synergies and to propose interoperable approaches. Powers and mandates are discussed in this context, as well as the necessity to build upon the SDGR OOTS in the context of the Data Spaces.

It would be very useful, in the opinion of the project partners, to move towards a more agile and permanent legal framework for cross border eGovernment in the EU in general, that could more easily be extended to integrate existing building blocks, but also to cover new procedures, new legal requirements, new information exchange patterns, or new paradigms to determine the authenticity and reliability of government issued information. This would allow all outputs of the DE4A project to be integrated, sustained and expanded, without requiring ad hoc legal interventions that risk creating new layers of complexity, or creating real or perceived inconsistencies.

Annex I - DE4A Legal Sustainability Workshop – context and minutes

Introduction

The objective of D7.4 is to provide recommendations on how to ensure the sustainability of DE4A outputs from a legal perspective. To the extent that DE4A builds on the SDGR, this will entail an explanation of the governance and sustainability mechanisms foreseen in the SDGR and its IR, and an explanation of how DE4A outputs fit in.

However, there are a number of topics for which the outputs don't fit neatly or perfectly into the SDGR/IR context. The DE4A consortium agreed to try to provide suggestions on how these can be sustained as well – within the SDGR, within other legislation (eIDAS 2, Data Governance Act, Data Act), or via new initiatives. To discuss potential topics, a workshop on legal sustainability was held online.

Attendance and logistics

The Workshop was held via a Teams call on 12 January 2023, from 14h to 15h40 CET.

The following persons participated:

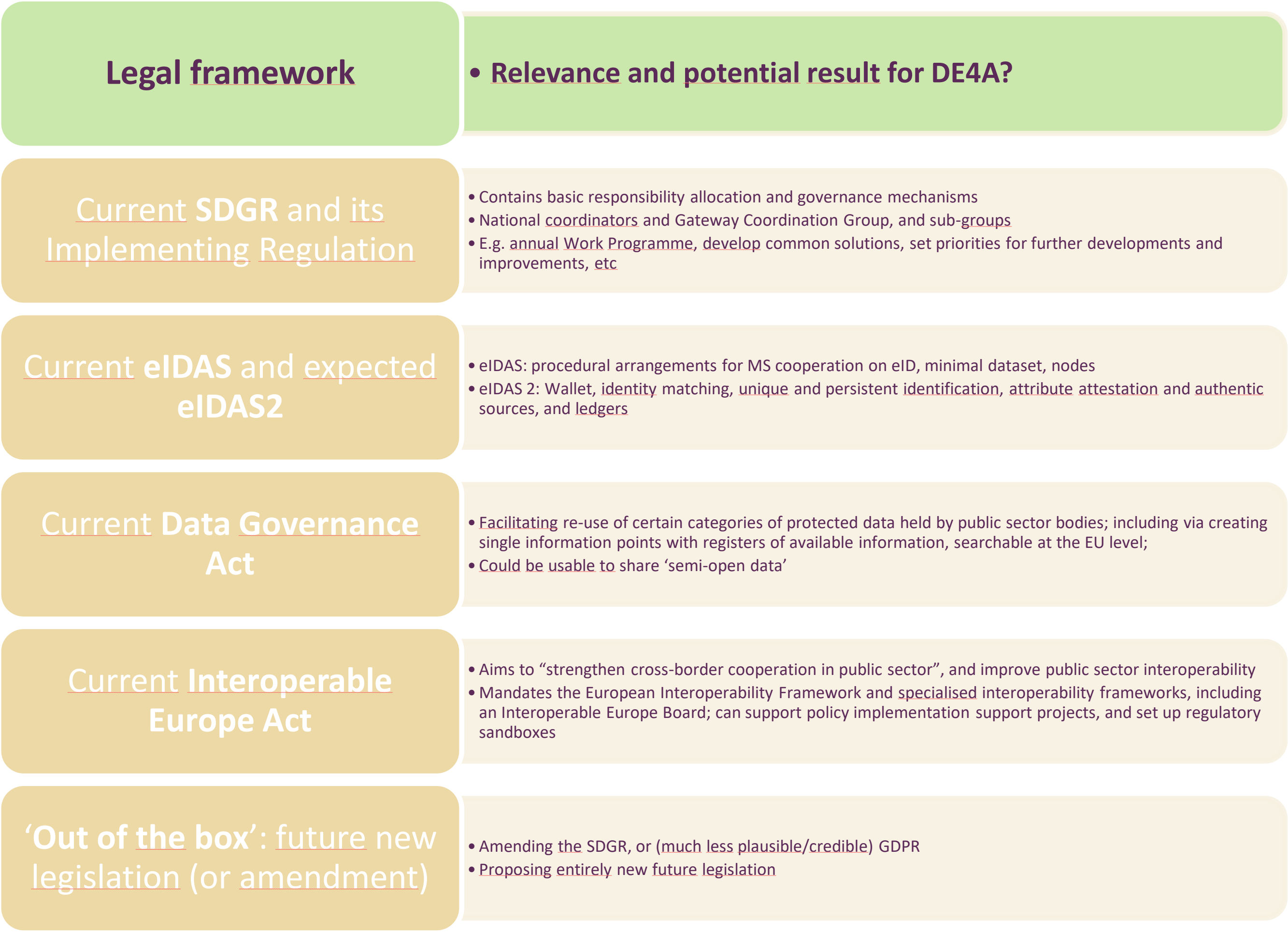
- Hans Graux
- Fredrik Linden
- Arvid Welin
- Ivar Vennekens
- Ana Maria Piñuela Marcos
- Ana Rosa Guzman Carbonell
- Norlander Malin
- Alexander Bielowski
- Alberto Crespo
- Tomaz Klobucar
- Bart van Bekkum
- Gérard Soisson
- Francisco José Aragó Monzonís
- João Matos
- Javier Ferrero Merchán
- Miha Jesenko
- Tiago Catarino
- Kapantai Eleni
- Muhamed Turkanović

Report and minutes

Introduction

Hans Graux introduced the objective: suggesting legal sustainability options that exceed the current legal framework, and that exceed DE4A's scope and capabilities.

The main legal modalities for providing legal sustainability to DE4A outputs were briefly summarised as follows:



Legal framework	• Relevance and potential result for DE4A?
Current SDGR and its Implementing Regulation	• Contains basic responsibility allocation and governance mechanisms • National coordinators and Gateway Coordination Group, and sub-groups • E.g. annual Work Programme, develop common solutions, set priorities for further developments and improvements, etc
Current eIDAS and expected eIDAS2	• eIDAS: procedural arrangements for MS cooperation on eID, minimal dataset, nodes • eIDAS 2: Wallet, identity matching, unique and persistent identification, attribute attestation and authentic sources, and ledgers
Current Data Governance Act	• Facilitating re-use of certain categories of protected data held by public sector bodies; including via creating single information points with registers of available information, searchable at the EU level; • Could be usable to share 'semi-open data'
Current Interoperable Europe Act	• Aims to "strengthen cross-border cooperation in public sector", and improve public sector interoperability • Mandates the European Interoperability Framework and specialised interoperability frameworks, including an Interoperable Europe Board; can support policy implementation support projects, and set up regulatory sandboxes
'Out of the box': future new legislation (or amendment)	• Amending the SDGR, or (much less plausible/credible) GDPR • Proposing entirely new future legislation

Figure 2: DE4A legal workshop topics overview

Five topics were prepared for further presentation and discussion, stressing that participants should be feel to suggest others, during the workshop or afterwards.

1. Subscription and notification
2. The role of mobile wallets
3. Credentials / VCs (including revocation)
4. Fine-grained powers and mandates / powers catalogue
5. Rights of representation

Various proposals were provided:

- As an additional suggestion, it was noted that we should also discuss the data spaces concept, as supported by the Data Act and the Data Governance Act. How do we see the technical system fitting in there (if at all)? This should be acknowledged as a sustainability option for our work too (e.g. via an e-government data space).
- Moreover, the first topic (subscription and notification) should be renamed 'multi-pattern approach'. This is an enhancement we developed in DE4A that was not present in the legislation, and it's important for the USI pattern, look-up, push-pattern, etc. Calling it subscription and notification is too constrictive, and doesn't allow the integration of 'pro-active' government, since once-only is reactive only now.

- Deregistration and interrupted procedures need to be integrated as well – either within the multi-pattern topic, or as an independent point.

Each of these was further discussed in turn, as summarized below.

Subscription and notification (to be renamed 'multi-pattern exchanges')

The issue is supporting exchanges without individual prior requests and previews (not unambiguously linked to the SDGR vision). As discussed during the introduction, this section will be broadened to 'multi-pattern exchanges' in general. We will explain that we support many other patterns, which are useful from a public policy perspective, but are not clearly supported in the legal framework now.

How can this be sustained?

- Under the current SDGR (without amendments), it is possible to define practices on the interpretation of the current legislation: e.g. clarification on what constitutes an 'evidence', or what exceptions are 'provided under Union or national law', or whether a 'request' can have an unlimited duration
- Alternatively: an out of the box solution, via an SGDR amendment, or entirely new legislation that supports multi-pattern exchanges explicitly, and defines safeguards (without emphasizing 'explicit request' so much). E.g. exchanges for the public interest (to combat fraud) could then be supported.

Feedback from the participants:

- The data spaces topic is very important as a potential solution here, with sufficient focus on interoperability. The current focus is very sector specific, and that can be dangerous, since we don't have a clear view on how interoperability between sectorial data spaces could be ensured. 'Meta-legislation' to address this point could be useful. Otherwise, data spaces will create new problems.
- eDelivery is a key building block for DE4A. We need stronger alignment on how to implement / use eDelivery in a homogeneous way.
- Both of those suggestions are broader than SDGR – it relates to eGovernment in general. The Interoperable Europe Act proposal is interesting in this regard, but not sufficient: the proposal focuses on governance, and we are talking now about operational implementation – a framework that allows hands-on work on this topic.
- Generally, 'out of the box' thinking seems to be required – this is not a pure SDGR issue, and shouldn't be treated as such. A transversal regulation to reduce administrative burdens for citizens and administrations might part of the solution, along with rules to operationally address interoperability – recognizing though that there is always a dependence on national laws (e.g. legislation on whether you can have two domiciles – and thus whether deregistration is required – is currently entirely national). An overall strategy for data exchanges – including our multi-pattern approach – with a supporting legal framework would be needed.
- D2.7 [28] should be considered as well when drafting this (especially concluding sections of that deliverable). Our project provides a very useful and effective architecture that can be used to support a potential future broader legal framework for a multitude of eGovernment exchanges – comprising governance, interoperability, and multi-pattern exchanges. That should be the 'horizontal' sustainability challenge.

Role of mobile wallets

The issue is that the SDGR is not really well attuned to Wallets – we can support it in DE4A, but there is some tension between once-only and Wallets: once-only focuses more on direct exchanges between administrations, whereas Wallets put citizens in charge.

How can this be sustained?

- Legislation: an explicit linkage in eIDAS 2 with the SDGR, to clarify that Wallets are usable to meet the SDGR requirements.
- Or via SDGR governance mechanisms, integrating the Wallet logic into the architecture
- Or out of the box / SGDR amendment?

Feedback from the participants:

- The tension is not really between once-only and Wallets, but between administration centric and citizen centric.
- The Implementing Regulation did at some point include a reference to the Wallets, but the reference was deleted from the final version since the eIDAS 2 amendment was not yet adopted. But Wallets are fully user-centric, so there shouldn't be a problem in principle.
- This issue is seen as less critical – Wallets are usable for the SDGR, that's not a particularly controversial topic.

Credentials / VCs (including revocation)

We've been asked by the reviewers to discuss this in particular. Credentials receive only very indirect coverage under the SDGR – you can assume that a VC can be used as an 'evidence' under the SDGR, but there's no specific statements. There's better coverage in eIDAS2, possibly, via the notion of attribute assertions. But neither the SDGR nor eIDAS 2 has clear statements on linking VCs to e.g. their issuance by competent authorities under the SDGR, or with respect to verification and revocation.

How can this be sustained?

- Either by introducing specific language linking eIDAS 2 with the SDGR (noting that attribute assertions can be used as evidences under the SDGR, which seems however difficult to do in a meaningful way.
- Or via SDGR governance mechanisms, clarifying how/when a VC can be an 'evidence', and what this means

Feedback from the participants:

- The reviewers considered VCs to be important to promote DE4A outputs, and asked for more details on revocation, in particular, so we do need to address that.
- Likely the best approach is to explain what's already possible, and how / under which conditions competent authorities could indeed issue VCs as evidence; and analysing the cases under which revocation could be needed (or inversely: how the provisions in relation to e.g. validation of assertions against authentic sources in the eIDAS2 proposal help to address the revocation problem, where it exists). Linkability to the real competent authority is a critical point here – the WC3 has proposed solutions for validation and refreshing of VCs, but the consumption and verification of authenticity (whether the source was competent to issue it) has not yet been addressed.

- There is also an expectation management issue – in the analogue world (paper evidences), this issue is entirely unaddressed – there is no verification of the competence of the source, or any revocation.

Fine-grained powers and mandates / powers catalogue and rights of representation

These topics were discussed together, for timing / efficiency reasons. The fundamental problem is that, at the EU level, there is no clear model for registering or validating representation competences. For company representation, general powers of representation exist *de facto* (see also SEMPER), but there is no supporting legal framework for it. The legal reality behind general powers is often a lot more complex, depending on the type of legal entity, the powers/competences involved, and the procedure.

A comparable issue exists for representation of individuals (e.g. parents representing children, or representation persons with severe mental impairments).

These are not SDGR/DE4A issues, but it could be useful to make some comments on this none the less.

How can this be sustained?

- Probably best via eIDAS2
- Or via the Interoperable Europe Act

Feedback from the participants:

- The eIDAS 2 notification framework would also cover mechanisms for powers validation; that can become a tool to validate company representation rights. There's also a specific workstream there already that is attempting to define a catalogue for more fine-grained powers validation in the context of the SDGR procedures in particular. That should be referenced and acknowledged as well.
- For the representation of persons however, there is indeed no clear solution. We can only flag this as problem that requires future reflection, maybe for an eIDAS 3, or in the context of other future legislation (possibly in the Interoperable Europe Act).

Next steps

Meeting minutes will be drafted and disseminated.

A structure for the deliverable D7.4 will be created and made available via the Wiki in the beginning of February; and feedback will be sought/invited in the course of February, in order to finalize the deliverable in early March.

The meeting ends at 15h40.

References

[1] Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications (Text with EEA relevance) http://data.europa.eu/eli/dir/2005/36/oj

[2] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market http://data.europa.eu/eli/dir/2006/123/oj

[3] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC Text with EEA relevance http://data.europa.eu/eli/dir/2014/24/oj

[4] Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC Text with EEA relevance, http://data.europa.eu/eli/dir/2014/25/oj.

[5] 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) (Text with EEA relevance), http://data.europa.eu/eli/reg/2016/679/oj

[6] Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (Text with EEA relevance.) http://data.europa.eu/eli/reg/2018/1724/oj

[7] European Data Protection Supervisor, Opinion 8/2017 on the proposal for a Regulation establishing a single digital gateway and the 'once-only' principle, https://edps.europa.eu/sites/edp/files/publication/17-08-01_sdg_opinion_en_0.pdf

[8] European Data Protection Board, Guidelines 05/2020 on consent under the Regulation 2016/679, adopted on 4 May 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[9] Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679, WP 260 rev.01 from the European Data Protection Board, https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025

[10] Kamraro. 'Responsible Research & Innovation'. Text. Horizon 2020 - European Commission, 1 April 2014. https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation.

[11] See https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation

[12] DE4A Consortium, D7.3 - Final Report on legal and ethical recommendations and best practices can be consulted via https://www.de4a.eu/_files/ugd/2844e6_5d28cb24c58b4cac9785d653c6cd07be.pdf (Accessed: 30/03/2023).

[13] DE4A Consortium, D10.2 POPD Requirement n°2

[14] Commission Implementing Regulation (EU) (EU) 2022/1463 of 5 August 2022 setting out technical and operational specifications of the technical system for the cross-border automated exchange of evidence and application of the "once-only" principle in accordance with Regulation (EU) 2018/1724 of the European Parliament and of the Council; see https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2022%3A231%3AFULL&uri=uriserv%3AOJ.L_.2022.231.01.0001.01.ENG

[15] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity; see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A281%3AFIN

[16] Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity; see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[17] Proposal for a Regulation of the European Parliament and of the Council laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act), COM(2022) 720 final; see https://commission.europa.eu/system/files/2022-11/com2022720_0.pdf

[18] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A European strategy for data, COM/2020/66 final; see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066

[19] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) ; see http://data.europa.eu/eli/reg/2022/868/oj

[20] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final; see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN

[21] Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework; and Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means; see https://ec.europa.eu/futurium/en/content/eidas-implementing-acts.html

[22] Commission Implementing Decision (EU) 2015/296 of 24 February 2015 on procedural arrangements for MS cooperation on eID; see https://ec.europa.eu/futurium/en/content/eidas-implementing-acts.html

[23] Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists; Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies; and Commission Implementing Decision (EU)2016/650 of 25 April 2016 laying down standards for

the security assessment of qualified signature and seal creation devices; see https://ec.europa.eu/futurium/en/content/eidas-implementing-acts.html

[24] European Digital Identity Wallet Architecture and Reference Framework v1.0; see https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

[25] Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU; see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R0858

[26] Ministerial Declaration on eGovernment - Tallinn declaration; see https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration

[27] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a strengthened public sector interoperability policy - Linking public services, supporting public policies and delivering public benefits Towards an 'Interoperable Europe', COM(2022) 710; see https://commission.europa.eu/system/files/2022-11/com2022710_0.pdf

[28] DE4A Consortium, D2.7 – Interoperability Architecture for Cross-border Procedures and Evidence Exchange in light of the Single Digital Gateway Regulation, can be consulted via https://www.de4a.eu/_files/ugd/b332f5_f330437d87cb43beb7b35c660b9706fc.pdf (Accessed 31/03/2023)