
# D7.3 Final Report on legal and ethical recommendations and best practices

| Document Identification | | | |
|---|---|---|---|
| **Status** | Final | **Due Date** | 30/09/2022 |
| **Version** | 1.0 | **Submission Date** | 30/09/2022 |

| | | | |
|---|---|---|---|
| **Related WP** | WP7 | **Document Reference** | D7.3 |
| **Related Deliverable(s)** | WP4, WP7, WP8, WP9 | **Dissemination Level (*)** | PU |
| **Lead Participant** | Timelex | **Lead Author** | Hans Graux (Timelex) |
| **Contributors** | | **Reviewers** | Fredrik Lindén (SU) |
| | | | Gérard Soisson (CTIE) |

| **Keywords :** |
|---|
| Ethics, legal, requirements, compliance, SDGR, GDPR |

# Document Information

| List of Contributors | |
|---|---|
| Name | Partner |
| Hans Graux | Timelex |
| Pedro Demolder | Timelex |

| Document History | | | |
|---|---|---|---|
| Version | Date | Change editors | Changes |
| 0.1 | 1/06/2022 | Hans Graux (TLX) | Initial version of document |
| 0.5 | 15/08/2022 | Hans Graux, Pedro Demolder (TLX) | Initial analysis |
| 0.7 | 31/08/2022 | Hans Graux (TLX) | Addition of pilot experiences and best practices |
| 0.8 | 08/09/2022 | Hans Graux (TLX) | Adding analysis of the Implementing Act |
| 0.9 | 14/09/2022 | Hans Graux (TLX) | Finalisation for internal validation |
| 0.96 | 29/09/2022 | Hans Graux (TLX) | Integration of feedback from Fredrik Lindén (SU) and Gérard Soisson (CTIE) |
| 0.97 | 29/09/2022 | Hans Graux (TLX) | Final version |
| 0.98 | 29/09/2022 | Julia Wells (ATOS) | Final check for submission |
| 1.0 | 30/09/2022 | Ana Piñuela (ATOS) | Final version for submission |

| Quality Control | | |
|---|---|---|
| Role | Who (Partner short name) | Approval Date |
| Deliverable leader | Hans Graux (Timelex) | 29/09/2022 |
| Quality manager | Julia Wells (ATOS) | 29/09/2022 |
| Project Coordinator | Ana Piñuela Marcos (ATOS) | 30/09/2022 |

# Table of Contents

# List of Tables

# 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 Catalog Vocabulary |
| DE4A | Digital Europe for All (this project) |
| DEP | Digital Europe Programme |
| 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 (not yet published in the Official Journal) |
| 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 |
| 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 |
| TBW | To Be Written |
| TOGAF | The Open Group Architecture Framework, https://www.opengroup.org/togaf |
| TOOP | The Once Only Project, http://www.toop.eu/ |
| VC | Verifiable Credentials |

# Executive Summary

This deliverable is the third and final formal output of WP7 (Legal and ethical compliance and consensus building) for the DE4A project. It aims to summarise the legal and ethical compliance activities undertaken in the course of the project, including any recommendations, final texts, and legal and ethical best practices implemented in the project, in particular in the course of piloting activities.

It also provides inputs for future legal and policy actions under the Single Digital Gateway Regulation, and highlights potential avenues for further legal action (as a part of the SDG, or more broadly in relation to e-government).

To avoid repetition, this deliverable does not aim to restate all legal and ethics analysis developed during the project. For more details on this analysis, reference is made to D7.1 Overview of legal and ethical requirements [16] and D7.2 Initial Report on legal and ethical recommendations and best practices [17].

The present report comprises two major sections:

- Firstly, it summarises the legal developments and resulting legal requirements since the submission of the previous WP7 deliverable D7.2, and describes how these affect DE4A. This relates principally to the adoption of the final Implementing Regulation (IR) of the Single Digital Gateway Regulation, which finalises the legal framework of the SDGR with respect to the technical system; and to the ongoing discussions related to the eIDAS 2 proposal (on EU Identity Wallets and ledger technology, among other topics).
- Secondly, it presents concrete lessons learned and outputs created during the project's execution, both in relation to the DE4A infrastructure in general, and to piloting in particular. This section captures the current state of play, and indicates how DE4A generally operates from a legal and ethical perspective. It also identifies topics that will require future policy discussion, and potentially future legislative action.

# 1 Introduction

## 1.1 Purpose of this document

The present document is the third 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 at the national and EU level, as well as ethics in general. WP7 activities will continue until the project's termination, and actions that will be undertaken after the submission of this deliverable will be described herein.

Complementary to that formal compliance objective, this WP also aims to formalise a working consensus between Member States participating in DE4A, ensuring that they have a common view on how legal and ethical requirements should be met.

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.

This document, as the last deliverable in WP7, summarises all legal and ethical compliance activities undertaken in the course of the project, including any recommendations, draft texts and templates created during the project, and practical guidance on legal compliance. The actions are driven principally from EU level legal restrictions – notably those resulting from the SDGR (such as the prior request, the preview functionality, or the required communications to the users), but also from the GDPR (such as the need for lawfulness, proportionality and privacy by design). Moreover, as will be described further in this deliverable, some additional requirements were identified during piloting based on national legislation.

An initial analysis of the applicable legal framework for DE4A was undertaken via D7.1 - Overview of legal and ethical requirements. Contents from that deliverable will not be repeated here, although a short summary of the main legal requirements will be provided to facilitate reading. A first overview of concrete legal and ethical support activities undertaken in the course of DE4A was provided in D7.2 – Initial Report on legal and ethical recommendations and best practices; this too will not be repeated in the present report.

However, a key challenge for WP7 – and for DE4A as a whole – has been the uncertainty surrounding the legal framework, and on potential future policy evolutions. With respect to the legal framework, it is particularly worth noting that the SDGR was expected to be completed via secondary legislation – via a so-called Implementing Regulation (IR) – by 12 June 2021, to set out the technical and operational specifications of the technical system. While significant advances were made by that deadline and draft texts were circulated, the adoption of the final IR [13] was ultimately delayed until June 2022; it was signed on 5 August 2022, and published in the Official Journal on 6 September 2022.

A second challenge is that the remit of DE4A is not purely to implement and pilot the SDGR, but to explore generally how once-only functionality can be embedded into efficient digital government services in general. Alternatives to the perspective of the SDGR have been considered, and as will be commented below, DE4A has indeed explored alternative evidence exchange patterns. These raise new legal and ethical concerns and opportunities, which also should be addressed in DE4A, since they may feed into future EU or national level policies. Partially, these are affected by the recent proposal

for an amendment of the eIDAS Regulation [14], which proposes a legal framework for (among other topics) European Digital Identity Wallets and digital ledgers/blockchain technology. The eIDAS 2 amendment however remains at the proposal stage for now, so that it cannot provide conclusive legal solutions for the DE4A project.

As foreseen in the Grant Agreement, the current document contains an overview of these evolutions and their impacts, and summarises the legal and ethical compliance outputs and interpretations in DE4A at the time of submission.

## 1.2 Structure of the document

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

- Chapter 2 – General outline of the legal and ethical requirements of the SDGR and of the IR. This chapter summarises the essence of the SDGR, and also explains the relationship between the SDGR and DE4A. Most notably, it explains why the SDGR is not the sole legal and ethical driver behind DE4A. It also contains an analysis of the content and impact of the IR, and of the potential significance of the eIDAS 2 proposal (as it relates to the SDGR and DE4A).
- Chapter 3 – Legal and ethical actions undertaken, and lessons learned. This chapter describes the measures already undertaken in DE4A, including both actual sample texts provided, and the reasoning behind the texts. Lessons learned are described both at the project level, and for individual pilots.
- Charter 4 – Conclusions. This chapter outlines the main findings, and lists further support actions planned in WP7. It also identifies an initial list of potential follow-up actions outside the context of DE4A (i.e. for national and EU level policy makers and legislators).

# 2 General outline of the legal and ethical requirements

DE4A aims to comply with any relevant legal and ethics requirements. A key building block is of course the SDGR, as the main legal instrument governing the once-only principle at the EU level, and regulating the exchange of evidences between Member States for procedures falling within the scope of the SDGR. This second chapter of the deliverable briefly describes the requirements of the SDGR and its very recently adopted IR. It also explains why and to what extent the SDGR is not the only driver for legal and ethical requirements, and assesses the potential impact of the eIDAS 2 proposal.

## 2.1 The SDGR and its perspective on the OOP and Article 14

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 European Union, 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]. 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. DE4A in practice pilots a potential blueprint for this technical system.

With respect to scoping, under the SDGR, evidence that is relevant for the online procedures mentioned above must be made available to competent authorities in other Member States when:

- They are lawfully issued by the competent authorities, and
- They are issued in an electronic format that allows automated exchange.

Finally, article 14 stipulates that the envisaged technical system must contain certain features:

- The user must be able to explicitly request an exchange of evidence;
- It must enable requesting evidence,
- It must allow the automated transmission of electronic evidence between competent authorities of different Member States;
- It must allow the processing of the evidence by the authority that requested it;
- The confidentiality and integrity of the evidence must be ensured;
- The user must be able to preview the evidence before its exchange to the competent authority, and the user must be able to prevent the exchange if necessary;
- The system must be interoperable with other relevant systems;
- The exchange of evidence must be secure;
- The processing must be limited to what is technically necessary to ensure the exchange of evidence and the evidence must not be stored or processed if it is not necessary for the transfer.

The use of the technical system under the SDGR must be an option – a choice – for the user, who must always be permitted to choose not to use it if he prefers, and provide the evidence in an alternative manner (whether electronic or not). Moreover, the use of the technical system must be 'explicitly

requested' by the user; it cannot be the default mode of transfer of evidence[1]. Therefore, other means must be available for the user to submit evidence. However, the use of the technical system may be required by applicable national or EU law (i.e. other than the SDGR). The user must have the possibility to preview the evidence transferred unless EU or national legislation specifically provide for exchange without preview of the evidence. The evidence transfer must be limited to what is necessary for the administrative procedure at hand and may only be used for the purpose of the procedure at hand. The evidence thus obtained must be considered authentic evidence by the receiving competent authority.

Globally, the SDGR reflects a specific perspective on the OOP, and contains legal and ethical requirements that are driven by that perspective. As the recitals to the SDGR themselves describe it:

> *(44) In order to further facilitate the use of online procedures, this Regulation should, in line with the 'once-only' principle, provide the basis for the creation and use of a fully operational, safe and secure technical system for the automated cross-border exchange of evidence between the actors involved in the procedure,* ***where this is explicitly requested by citizens and businesses****. Where the exchange of evidence includes personal data, the request should be considered to be explicit if it contains a freely given, specific, informed and unambiguous indication of the individual's wish to have the relevant personal data exchanged, either by statement or by affirmative action. If the user is not the person concerned by the data, the online procedure should not affect his or her rights under Regulation (EU) 2016/679. The cross-border application of the 'once-only' principle* ***should result in citizens and businesses not having to supply the same data to public authorities more than once****, and that it should also be possible to use those data at the request of the user for the purposes of completing cross-border online procedures involving cross-border users. For the issuing competent authority, the obligation to use the technical system for the automated exchange of evidence between different Member States should apply only where authorities lawfully issue, in their own Member State, evidence in an electronic format that makes such an automated exchange possible.*

The OOP under the SDGR is thus driven by user requests. The SDGR in principle does not envisage transfers between competent authorities without user involvement (through explicit requests and previews), unless there is a separate legal basis to do so. Even in situations where automated exchanges would benefit the users (e.g. by automatically granting them financial benefits such as subsidies) or where automated exchanges would be in the public interest (e.g. by making it easier to detect fraud), the SDGR does not provide a legal basis for exchanges without user involvement or specific legislation requiring such exchanges. The SDGR therefore reflects a legal and ethical choice to support only a specific type of once-only information exchanges – notably those driven by a user request.

The choice is of course defensible from a policy perspective, but it also implies that other types of once-only exchanges – such as those proactively granting benefits to citizens without their request, or those enabling detection of errors or fraud without citizen intervention – are not explicitly supported by the SDGR. DE4A none the less also takes these situations into consideration and has created pilots around them, as will be explained below. Moreover, since all exchanges are user driven, the user must be identified reliably during the request process, so that they can be linked to the appropriate evidence. For this purpose, the SDGR relies on the legal framework of the eIDAS Regulation, which causes some practical and legal challenges, as will be explored in Section 2.4 below.

[1] However, piloting initiatives in DE4A only aim to test the implementations of the once-only principle and are not representative of final e-government services. For that reason, the pilot services are offered as digital-only and once-only by default, rather than as an additional option next to a paper process.

## 2.2 Requirements for the technical system under the SDGR and the Implementing Regulation

### 2.2.1 Requirements in the SDGR

Article 14 sets out several general legal requirements for the technical system envisaged by the SDGR. Some of these requirements are general features applicable to all transfers (e.g. security and safety of the evidence and its exchange, or data minimization to ensure proportionality), whereas some requirements relate only to features that may not be relevant in certain situations (e.g. the explicit request of the user and preview mechanism, both of which are subject to exceptions as will be outlined below).

- Enable the **request of evidence by a competent authority** to the another: the competent authority must be able to request evidence necessary for the completion of an administrative process from an authority holding such evidence.
- Support **explicit request of user** (i.e. citizens and private entities): the user must have the capacity to request that the evidence which is necessary for an administrative procedure is transferred through the technical system.
- Enable the **transfer of evidence**: the system must allow the transmission of evidence between competent authority.
- Allow the **processing of evidence**: the requesting authority must be enabled to process the received evidence. It is worth noting that the SDGR does not set out how such processing should take place.
- Ensure **adequate security** features: the evidence must keep its integrity and remain confidential.
- Support the **preview** of evidence: the user must have the possibility to preview the evidence they requested before its transfer, unless EU or national legislation explicitly provides this is not necessary.
- Enable the **data minimisation** principle: data must not be processed beyond what is technically necessary for the exchange, nor stored longer by the technical system than necessary for the exchange.

While some of these requirements are relatively trivial, others have more far reaching implications. Moreover, many of them required further elaboration through a specific IR. The contents and impacts of this IR will be briefly summarised below.

### 2.2.2 Requirements in the Implementing Regulation

Article 14.9 of the SDGR already noted that, by 12 June 2021, the Commission should "*adopt implementing acts to set out the technical and operational specifications of the technical system necessary for the implementation of this Article*". Proposals for an implementing act were circulated prior to this deadline, but failed to be adopted on time for a variety of reasons (including but not limited to discussions on scoping, supported exchange patterns, level of detail, and the governance mechanisms foreseen in the draft act).

After a so called right to scrutiny procedure was invoked by the Council of the EU in July 2021, discussions were continued, and a finalised act (an Implementing Regulation – IR) was adopted in June 2022, and published in September 2022 [13]. Its contents can be briefly summarised as follows, without endeavouring to go into exhaustive detail.

The IR essentially further outlines several architectural choices made in relation to the SDGR technical system. Specifically, it defines a series of common services at the EU level, and a series of Member State level services (all described in Articles 3 and following).

The common services comprise:

- a data service directory, containing a list of competent authorities acting as evidence providers, a list of available evidences, and semantic data; as well as identification requirements imposed by the Member States for accessing these evidences;
- an evidence broker, in charge of determining equivalence between evidences between Member States;
- a semantic repository, which identifies data models, associated schemata and data formats for each type of evidence.

The Member State services comprise:

- the procedure portals of competent authorities that require evidences (evidence requesters) or and the data services of competent authorities that issue evidences (evidence providers);
- intermediary platforms for providers/requesters that connect to common services. This is an optional component that allows Member States to build an intermediary between the technical system and certain competent authorities, in order to avoid that a very large number of sometimes smaller organisations are required to all maintain the relevant infrastructure individually;
- any national registries and services that are equivalent to the EU data service directory or broker, i.e. that Member States may choose to build to identify relevant authorities, evidences and equivalences at the national level; these must be either accessible to Member States, or copied to the EU data service directory or broker;
- eIDAS nodes for user authentication and identity matching, i.e. the services that allow citizens to identify themselves both towards the evidence issuers and evidence recipients (see also section 2.4 on identification and authentication below)
- eDelivery Access Points, i.e. standardised infrastructure to send or receive evidence, which must be used for providers/requesters/intermediaries;

Collectively, these components make up the once-only technical system, together with the procedure portals of evidence requesters and the data services of evidence providers, and the preview spaces.

The legislative framework is thus relatively prescriptive in terms of architecture, and the mandatory functionalities of these architectural components (such as e.g. the mandatory connection to eIDAS nodes and eDelivery Access Points, or the obligation for Member States to contribute to the information stored in the data service directory and the evidence broker).

In terms of supported exchange patterns, the initial drafts of the IR favoured the use of the intermediation pattern only, in which the user would only interact directly with the evidence requester, but not with the evidence provider(s). However, in subsequent negotiations, the IR was modified to support the user-supported intermediation pattern, by allowing direct interactions between the user and the evidence provider, as will be explained below. Identity matching is facilitated, as the responsibility is largely moved away from the evidence provider, thus reducing the chance of errors, and making it easier for data providers build on existing national means of identification. In this way, the IR is also more in line with the experiences of the DE4A project.

Beyond that, the IR also defines further legal safeguards that aim to ensure that the system will work as envisaged by the SDGR. Specifically (and simplifying somewhat):

- Article 9 provides further transparency obligations on the evidence requesters, including the duty to point out the voluntary use of the system, and the possibility to preview the evidence.
- Article 10 allows users to granularly select which evidence they wish to provide via the technical system.
- Article 11 acknowledges both the mandatory support for eIDAS notified eIDs, but also the right of evidence providers to request additional identity attributes before making evidences available.

- Article 12 requires the evidence requester to disclose both the names of evidence providers, and the evidence types that will be exchanged.
- Article 15 further defines the evidence exchange flow under the SDGR, noting principally that the preview space for evidences must be foreseen at the evidence provider side, or with an intermediary platform.
- The redirection of the user to the evidence provider for previewing purposes was integrated in article 14, and the right for evidence providers and intermediaries to request reidentification and/or additional attributes if necessary to allow identity matching is outlined in Article 16, along with the obligation to return error messages if the matching fails. These articles provide support for the user-supported intermediation pattern, since it explicitly allows interaction between the user and the evidence provider. While this implies potentially slightly greater effort for the user compared to the theoretically simpler intermediation pattern, it does significantly increase the accuracy of the identification and identity matching. Moreover, since evidence previewing occurs at the evidence provider's side, no exchange of the evidence occurs prior to the preview possibility. This is a superior choice from a data protection perspective, since evidence is not needlessly made available to a third party.
- Logging obligations are set out in Article 16; and governance mechanisms in Articles 18 and following.
- Finally, SLA targets are set out in Article 27, specifying an operating time frame of the technical system in its entirety of 24 hours a day/7 days a week, with an availability rate of the eDelivery access points, preview spaces and common services of at least 98 % excluding scheduled maintenance. Individual components of the OOTS may have different SLA targets, that can be defined through the governance processes described in the IR.

Thus, the IR is relatively prescriptive in terms of scoping, safeguards, governance and architectural logic; but relatively abstract with respect to actual standards, protocols and data formats.

## 2.3 OOP, DE4A and e-government beyond the SDGR

One of the objectives of DE4A is to establish piloting solutions for the technical system as envisaged by the SDGR and the IR. For that reason, the requirements established by Article 14 of the SDGR and in the subsequent IR are important inputs to determine the legal constraints for the DE4A project, notably because its piloting applications largely fall within the scope of the SDG online procedures.

However, as will be explored in greater detail in the following sections, there is no perfect alignment between DE4A's activities and the SDGR/IR (although this has improved with the IR's explicit support for user-supported intermediation). DE4A also aims to explore alternative solutions to once-only functionality or to efficient e-government services in general, with other interaction patterns that may go beyond the SDGR/IR requirements.

A key example is the case of proactive, automated or recurring evidence exchanges, which are not individually driven by a new request, and do not involve a new preview for each individual exchange. These exchanges would e.g. enable proactive rights granting, or automated error and fraud detection, without user request. Such exchanges can be beneficial from a public policy perspective, but do not fall perfectly in line with the OOP-perspective of the SDGR. DE4A pilots these patterns, but as will be explained below, specific safeguards and constraints are implemented. DE4A supports a lookup function that allows an authority to consult publicly available information, but since this information is publicly available, it is exempt from the prior request requirement. Additionally, DE4A will also pilot a subscription and notification pattern, which however only exchanges information that indicates whether evidence has changed – no evidence as such is exchanged without a prior request.

A second example is the use of so-called verifiable credentials (VC): electronic documents which are signed and authorised by a trusted issuer, which are requested and received by the citizen to whom it relates, and which can thereafter be made available to any party selected by the citizen. This too is an approach that offers clear added value, since it grants citizens sovereignty over their own data. However, the approach is not a direct application of the OOP as envisaged by the SDGR, since it requires the holder of the verifiable credential – the citizen – to control the exchange, rather than relying on a direct exchange between competent authorities.

These use cases may not fall entirely within the boundaries of the SDGR, meaning that piloting activities using these exchange patterns may not have a clear legal basis in the SDGR, and present legal and ethical challenges that transcend the limits of the SDGR. None the less, with a view to evolving towards optimal e-government services (a.k.a digital government), the DE4A project pilots these patterns, to the extent that this can be lawfully done. For that reason, this report not only explains how the legal and ethical requirements of the SDGR are adhered to, but also explains more broadly how legal and ethical requirements are addressed, even outside the context of the SDGR.

## 2.4 Identity, authenticity, integrity and the eIDAS 2 proposal

A critical element in any once-only exchange is that the identity of the participants can be determined. This includes the user (the person triggering the exchange, either on behalf of themselves or acting on behalf of an identified legal entity), but also the evidence requester, evidence provider, and other roles defined in the SDGR and in the IR. Moreover, their legal capacity to act in the specific procedure must be verifiable (e.g. a user's competence to represent a legal person, an evidence provider's right to demand certain evidences for certain procedures, and the legal authority of the evidence issuer), and the integrity of the exchanged information must be ensured (i.e. it must be assessable that the information has not been modified or otherwise corrupted since its issuance or creation).

To some extent, these requirements are regulated by the SDGR, which defines some of the underlying roles and responsibilities, and clarifies the means of identification and authentication that must be used. For instance, the evidence broker and data services directory are precisely intended to map the relevance and authenticity of specific evidences for specific procedures, and to identify which authorities may act as requesters and/or providers of those evidences. Specific infrastructure is thus foreseen and regulated to support the identification and validation of providers, requesters and evidences.

However, the SDGR also calls upon other legislation, notably the eIDAS Regulation [15]. This 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. At a high level, the eIDAS Regulation allows Member States to notify electronic means of identification used by the public sector (e.g., eID cards or mobile identification apps), and to allow an objective assessment of the reliability of those means of identification on the basis of common EU standards (their so-called level of assurance, which can be rated as high, substantial, or low). Once the notification and assessment is completed, citizens holding those means of identification can use them to access e-government services in other Member States, provided that their means of identification offers at least the same level of assurance as required domestically – i.e. a Member States that allows its own citizens to log onto an e-government application with means of identification at the substantial level, must also allow other EU

citizens to log on if they use a notified means of identification that are similarly at least substantial in quality.

The eIDAS Regulation 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:

- Electronic signatures allow natural persons to sign electronic information;
- Electronic seals allow companies and administrations to ensure the integrity and authenticity of electronic information;
- Timestamps allow the objective determination that a certain piece of electronic information existed at a specific moment in time;
- Electronic registered delivery allows anyone to exchange electronic information securely and confidentiality, in a manner that allows the identity of the sender and recipient to be validated, as well as the time of sending and receipt.

The SDGR already referenced these building blocks to a limited extent, noting in recital (21) that "*This Regulation should build on Regulation (EU) No 910/2014 of the European Parliament and of the Council (13), which lays down conditions under which Member States recognise certain electronic identification means for natural and legal persons subject to a notified electronic identification scheme of another Member State. Regulation (EU) No 910/2014 lays down the conditions subject to which users are permitted to use their means of electronic identification and authentication to access online public services in cross-border situations. Union institutions, bodies, offices and agencies are encouraged to accept means of electronic identification and authentication for the procedures for which they are responsible*". Recital (49) added that "*A number of building blocks offering basic capabilities exist that can be used to set up the technical system, such as the Connecting Europe Facility, established by Regulation (EU) No 1316/2013 of the European Parliament and of the Council (23), and the eDelivery and eID building blocks that form a part of that facility. Those building blocks consist of technical specifications, sample software and supporting services, and aim to ensure interoperability between the existing information and communication technology (ICT) systems in different Member States so that citizens, businesses and administrations, wherever they are in the Union, can benefit from seamless digital public services*".

The eIDAS Regulation as such was not explicitly referenced in article 14 of the SDGR itself, which describes the requirements for the technical system. The Regulation is however integrated into OOP procedures via article 13, 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-crossborder 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.

Thus, the SDGR and eIDAS Regulation are relatively well aligned. None the less, the solution does not comprehensively address all legal challenges encountered in DE4A. Three categories of challenges are encountered in particular:

- Firstly, the issue of identity mapping, i.e. the linking of a specific user to a specific evidence, as held by an evidence provider. This could be trivial if the evidence provider would use the same unique identifiers used by the identification scheme of the eIDAS eID. In reality however, that's virtually never the case, especially in the cross border contexts targeted by the SDGR, where the data requester and data provider are typically established in different Member States and do not rely on the same unique identifiers.

  The IR solves this issue in article 16 by allowing the evidence provider to request a new reidentification/reauthentication, and allowing them to request additional identity attributes. In this way, they can request that the eIDAS based identification triggered through the evidence requester is enriched with nationally used identifiers that the evidence provider relies on. If the user is already known nationally, such a national identifier from the evidence provider's country should be available, and evidence retrieval is a relatively simple matter of looking up the user's evidence on the basis of that identifier. This enables the eIDAS framework to build on any identification system already in use nationally (whether it is eIDAS notified or not). Inversely, if the user is not yet known (e.g. because it is his/her first interaction in that country), an onboarding process can first be done to create a national identifier.

  This approach implies that the matching to be done by the evidence provider under article 16.2 of the IR is not directly based on the eIDAS minimal data set, but linked to national identity attributes which have not necessarily been assessed under the eIDAS Regulation. Moreover, when the user is not yet known nationally, either a new onboarding process has to be created, or identity matching has to be done without unique identifiers. The latter is always an uncertain process, and discouraged by the IR's article 16.3, which notes that "*Where the process of identity and evidence matching does not result in a match or the identity matching generates two or more results, the user or the representative where applicable shall not be allowed to preview the requested evidence and the evidence shall not be exchanged*".

  In legal and practical terms, the main consequence is that the nationally used systems can be leveraged more effectively for the SDGR context. This is the approach of the user-supported intermediation pattern, which is also used in several DE4A pilots.

- Secondly, the problem of **representation**. The user of the technical system doesn't necessarily act on their own behalf, or at least not exclusively. They may act on behalf of a legal entity, or in some procedures they can act on behalf of other persons (e.g. their household members). Neither the eIDAS Regulation nor the SDGR has a comprehensive solution for this problem. While the eIDAS Regulation does provide a legal framework for the representation of legal entities, and defines a minimal data set for legal entity data that must be available via the nodes, under EU law there is no standardised solution to determine the legal competences of a representative of a legal entity. The same applies also for the representation of other natural persons (e.g. of one's children): there is no EU level legislation to determine the verifiable legal value of a person's claim to legal representation rights over another individual. This implies e.g. that the current legal framework can support individual persons moving from one Member States to another, but their ability to also change the official domicile of their children cannot be verified automatically at this stage.

  The SDGR and the IR do not settle this issue. They do acknowledge that persons may act on their own behalf or through a representative; and recital (21) of the IR notes that "*certain procedures are relevant for businesses, and entrepreneurs should therefore be able to request the exchange of evidence either on their own behalf or through a representative. [The eIDAS Regulation] provides a trusted legal framework for electronic identification means issued for legal persons or for natural*

*persons representing legal persons. The mutual recognition of national electronic identification means under that Regulation applies to these cases of representation. This Regulation should therefore rely on Regulation (EU) 910/2014, and any implementing acts adopted on its basis, for the identification of users in cases of representation. The gateway coordination group and its subgroups should cooperate closely with the governance structures established under [the eIDAS Regulation] to help develop solutions for powers of representation and mandates. Given the reliance of some of the procedures covered by the OOTS on the framework created by Regulation (EU) 910/2014, pieces of evidence requested by representatives should also be able to be processed through the OOTS when and to the extent to which these solutions will have been found*." Thus, the Regulation recognises that further work is required – and rightly stresses that the cooperation mechanisms to do so exist – but does not yet contain a viable solution.

- Finally, the issue of **verifiable credentials** and the role of individuals. The SDGR fundamentally relies on users as the gatekeepers of information exchanges relating to them: the users request evidence exchanges, and evidences are then exchanged between providers and requesters. However, the SDGR did not foresee a model where the users hold and manage their own information, e.g. in the form of verifiable credentials, stored in digital identity wallets or other secured storage spaces. No specific legal framework is built for this approach. That does not imply that it is not legally viable: evidence providers could issue verifiable credentials, relying on qualified signatures and seals regulated by the eIDAS Regulation, and there is no legal encumbrance for users to make these evidences available to requesting authorities. However, this model is not fully in line with the vision or the architectural current main model of the SDGR.

The eIDAS Regulation is however presently undergoing revision, and a proposal for an update to the eIDAS Regulation was published in June 2021 [14]. While this proposal is not limited to, or focused on the SDGR, it does aim to address some of the aforementioned gaps. 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

Wallets could also be technically standardised in a more consistent manner across the EU under the proposal. Thus, the Wallets potentially could become the principal access keys to public and private services in the EU.

This does, however, create a potential policy challenge for Member States, with the eIDAS revision more strongly referencing mobile data control (and data holdership) by individual citizens, and the SDGR focusing more on direct exchanges between competent authorities without data being retained by the users themselves. The combination is not incompliant, but does require further reflection on the best way forward for citizens and public administrations.

In the sections below, we will outline how DE4A addressed the requirements in practice, and what the main lessons learned were.

# 3 Legal and ethical actions undertaken, and lessons learned

## 3.1 General legal and ethical toolset of DE4A

During the preparation of the piloting activities, a range of legal and ethical tools were made available as a part of WP7 activities. These have been described at length in D7.2 – Initial Report on legal and ethical recommendations and best practices, and will not be reprised here. By way of a short summary however, this section will only provide a short overview of the tools, and provide an update on their actual use.

### 3.1.1 Ethics – data protection actions and templates

Within WP 10 (Ethics Requirements), a range of templates and procedures were developed. Their actual impact through WP 7 can be summarised as follows:

#### 3.1.1.1 D10.1 – Identification and consent scheme, providing templates for recruiting piloting participants

The general template privacy policy and consent statement from this deliverable was used as a starting point for two more concrete outputs:

- Privacy policies for the pilot specific pilot micro-sites on the general DE4A website;
- Summary language for the wireframe templates which were used for the development of the pilot applications.

In this way, the templates were used to develop a shared data Protection approach for all pilots. Since this improved coherence and transparency, this can be considered a good practice.

#### 3.1.1.2 D10.2 – Appointment of a Data Protection Officer

The role of the DE4A project DPO was to ensure alignment across the pilot streams with respect to data protection and data protection risk. This role could have been relatively minimal, since public administrations are required to have their own DPO under the GDPR, so that each partner's own DPO could have performed supervisory duties. In practice, however, as will be commented below, all partners opted to rely on the DE4A DPO as the primary point of contact. This facilitated coherent monitoring, and can therefore also be considered a good practice.

#### 3.1.1.3 D10.3 - Further processing of personal data

The processing of personal data beyond the initial purpose for which it was collected is 'further processing' in the sense of the GDPR. This deliverable examined to what extent further processing of pre-existing data would be permissible within the DE4A project.

In practice, the assessment was of little relevance, since all data processing in the piloting activities relied on primary data, i.e. data collected specifically for the purposes of the DE4A project. This was also the approach favoured explicitly in the deliverable, so this was not an unexpected fact. As a result, however, no 'further processing' in the sense of the GDPR actually occurred, so that the deliverable was not impactful in practice.

### 3.1.2 Wireframes, disclaimers, and privacy policies

A significant part of the legal and ethical requirements needed to be implemented through standardised communications towards pilot participants. This included:

- Commented wireframes, i.e. legal guidance on the language to be used in DE4A piloting procedures. These were aligned with the requirements of the SDGR, principally, and included references to the prior request and preview requirements;
- Standardised disclaimers, governing the legal assurances (or lack thereof) relating to the responsibilities and liabilities of piloting partners:
    - One variant addressed non-operational piloting (i.e. pilots using fake data; or using real data on non-operational systems). The key requirement for the use of this disclaimer is that the piloting cannot have any impact on real persons.
    - A modified piloting disclaimer for "live piloting", intended to be used for piloting with real data on operational systems. The key requirement for this disclaimer is that the piloting can have an impact on real persons.
- And finally, a template privacy policy, designed to be usable for operational and non-operational piloting cases.

All of these required instantiation and customisation based on the individual pilots. Microsites were maintained on a pilot stream basis, on which relevant disclaimers and privacy policies can be centrally maintained.

### 3.1.3 Ethical requirements and the DE4A Data Protection Impact Assessment

#### 3.1.3.1 Ethical requirements and fundamental rights in general

With respect to ethical requirements in general, the DE4A project is driven principally by the safeguards related to data protection as integrated into the GDPR, and by the safeguards aiming to protect the citizen as integrated into the SDGR. However, the scope of ethics and the scope of European values is broader than data protection and privacy alone. For this reason, a broader ethics assessment was completed via D10.5 – Periodic report by the independent Ethics Advisor, separate and independently from the DE4A DPO.

#### 3.1.3.2 The DE4A Data Protection Impact Assessment

Under European data protection law, specifically the GDPR, a DPIA must be conducted whenever "*a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons*". In such cases, prior to initialising the processing operations, the data controller(s) must carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

Keeping this in mind, and as recommended in the ethics reporting, a DPIA for the DE4A piloting activities was completed. As with any DPIA, this document was developed iteratively based on the suggestions and feedback of the DE4A partners. They have validated its contents after its completion. No updates or changes to the DPIA have been needed thus far.

### 3.1.4 Legal basis and commitments from the DE4A partners – the DE4A Memorandum of Understanding

Within DE4A, and similar to the approach taken in other Large Scale Pilot projects in the EU, a DE4A Memorandum of Understanding (MoU) was drafted, providing a joint statement of mutual understanding between piloting partners in relation to the requirements, assurances and limitations in relation to piloting. An MoU is not a legally binding contract. It is a non-binding, good faith, statement of shared understanding between the signatories.

The MoU implemented a risk based governance mechanism, requiring pilot participants to evaluate what the risk is in each piloting activity, and to take (and document) specific measures to mitigate these risks. In this way, a coordinated governance approach is created for all DE4A piloting activities.

While this took significant time and effort, all piloting partners ultimately provided a signed MoU prior to initiating piloting activities. As will be explained in the next section, this approach was built on to establish a data protection/ethics supervision scheme at the pilot specific level.

## 3.2 Implementation and experiences at the horizontal (non-pilot specific) level

The section above described the templates and supporting legal documents created in DE4A to facilitate compliance. However, these must also be adapted and used in practice. Even when no modifications are needed, some monitoring and evaluation is required to be able to confirm at any time that the defined requirements are adhered to. This section will describe how this was done in general, before proceeding to pilot specific findings in the next section.

### 3.2.1 Practical follow-up – data collection and documentation in DE4A

The template below was created within WP7 to keep track of the status of use cases in each individual pilot, and to register any legal issues encountered, along with implemented solutions. The template was disseminated via the project wiki and via e-mail, and was required to be applied at the use case level (not at the pilot stream level), registering the status for each country:

Use case status template

| ***Use case [name]*** | | | |
|---|---|---|---|
| ***Data provider country*** | | ***Data evaluator country*** | |
| **Member State name** | ***Status in this use case*** | ***Member State name*** | ***Status in this use case*** |
| [*Member State name*] | *Pick whichever one applies:*<br>*[not active yet] [issuing fake data] [issuing real data]* | *[Member State name]* | *Pick whichever one applies:*<br>*[not active yet] [receiving fake data] [receiving real data]* |
| [*Member State name*] | *Pick whichever one applies:*<br>*[not active yet] [issuing fake data] [issuing real data]* | *[Member State name]* | *Pick whichever one applies:*<br>*[not active yet] [receiving fake data] [receiving real data]* |
| ***Identified risks / problems / incidents*** | | ***Implemented solutions or plan*** | |
| *[Member State(s) name(s)]* | *Describe: dd/mm/yyyy, [description of the risk/problem/incident* | *Describe: dd/mm/yyyy, [description of the solution or plan]* | |

Table 1 : Use case status template

In addition to this use case template however, a separate template was needed to track whether pilot activities also respected the requirements defined in the DE4A Memorandum of Understanding, since otherwise the DE4A had no way of assessing to what extent piloting was legally compliant at any time. For that purpose, a second template was created, which was again disseminated via the project wiki and via e-mail:

MoU measures template

***a. Pilot risk status***

*Please tick the risk level of the pilot use case in the table below. As noted in the MoU:*

- ***Low risk** piloting activities include piloting activities that involve only fictitious persons, fictitious data, and test procedures. All three of these requirements must be met, or the piloting activities are qualified as medium risk.*
- ***Medium risk** piloting activities include piloting activities that involve any one or two of the following factors (but not all three cumulatively, since that would qualify as high risk):*
    - *Real-life persons*
    - *Real-life data*
    - *Production environments*
- ***High risk** piloting activities including piloting activities that cumulatively involve real-life persons, real-life data, and production environments.*

| ***Risk level*** | ***Tick if this level applies (tick only one)*** | ***Comments (if any)*** |
|---|---|---|
| *Low* | *[check or leave blank]* | *[optional - provide any information that may be needed to explain the risk level]* |
| *Medium* | *[check or leave blank]* | *[optional - provide any information that may be needed to explain the risk level]* |
| *High* | *[check or leave blank]* | *[optional - provide any information that may be needed to explain the risk level]* |

***b. Measures taken***

*Please tick and describe the measures taken to ensure compliance with the MoU:*

| *Measure description* | *Tick if this measure was taken* | *Description or comments (if any)* |
|---|---|---|
| *Piloting partners will **communicate proactively towards each other on issues or incidents** (**always mandatory**)* | *[check or leave blank]* | *[optional - describe how this is organised]* |
| *Any real-life **pilot participants (if applicable) are informed** of the fact that they are involved in piloting activities,*<br><br>*including any risks and countermeasures taken, and the (lack of) legal effects and consequences of participation.*<br><br>*Appropriate documentation should be retained to demonstrate that this information has been provided.*<br><br>***(mandatory for medium and high)*** | *[check or leave blank]* | *[Describe how this is organised]* |
| *If the piloting involves **real-life persons**, piloting should be organised under the **supervision of a DPO**.*<br><br>***(mandatory for medium and high)*** | *[check or leave blank]* | *[Identify the DPO]* |
| *If the piloting would be done on a **production environment**, all pilot partners should **notify** any operators of such environments in advance.*<br><br>*Appropriate measures should be taken that piloting activities d**o not result in negative legal or practical consequences** for any real-life persons, real life data, or production environments.*<br><br>*The production environments should be **cleaned** if the piloting activity was not intended to have long term legal or practical consequences.*<br><br>***(mandatory for medium and high)*** | *[check or leave blank]* | *[Describe how this is organised]* |
| *All piloting activities should be **monitored by pilot partners** (each solely in relation to such components of the piloting activities which are under their responsibility)*<br><br>*in a manner that allows any incidents to be detected and remedied (including by contacting any affected real-life persons where needed).*<br><br>***(mandatory for medium and high)*** | *[check or leave blank]* | *[Describe how this is organised]* |

| | | |
|---|---|---|
| *The **DE4A project DPO** (Hans Graux) should be informed prior to initiating piloting activity, and of any incidents that are reasonably likely to create legal effects or practical impacts on any real-life persons*<br>***(mandatory for high)*** | *[check or leave blank]* | *[Satisfied by sending an e-mail to the DPO]* |
| *Implementation of a **pilot monitoring and remediation strategy** to assess whether exchanged evidences are reasonably capable of satisfying the requirements for high risk piloting documented in the deliverables,*<br>*and to ensure that any errors in the piloting activity can be detected and remediated in a manner that eliminates any negative legal or practical consequences.*<br>***(mandatory for high)*** | *[check or leave blank]* | *[Satisfied by referencing the appropriate documentation describing the strategy]* |

Table 2 : MoU measures template

### 3.2.2 Supervision mechanisms and one-to-one alignment

The templates above were completed for all use cases (via the Wiki for the Use case status template, and via e-mail exchanges for the MoU measures template), and were updated from time to time, as required. This allowed the state of play to be followed for each use case.

The data collection also implied periodic follow-up by WP7, including via one-to-one meetings with pilot leaders, to verify that all information was accurate, completed and still up to date. With this approach however, the model was largely effective.

## 3.3 Implementation and experiences at the pilot specific level

### 3.3.1 Doing business abroad

#### 3.3.1.1 Summary of pilot specificities

This stream contains a combination of two use cases (Starting a business in another member state, and Doing business in another member state). The pilot focuses on businesses (i.e. legal entities) and is therefore somewhat less data protection sensitive, but they must of course be represented by natural persons. Therefore, the issue of representation and legal mandates (and the challenges identified in section 2.4) are particularly relevant for this pilot stream.

Four Member States are involved in piloting activities (Austria, the Netherlands, Romania and Sweden), and three patterns are involved: the Intermediation Pattern, the Subscription and Notification Pattern and the Lookup Pattern. Therefore, this pilot stream needs to examine the legal challenges (both with respect to GDPR and with respect to the SDGR for subscription and notification patterns, where new exchanges are triggered using the Lookup Pattern, without a new individual request from the user, and without preview functionality.

#### 3.3.1.2 Specific actions undertaken and lessons learned

Within this particular pilot stream, **extensive use was made of the provided templates**, which were kept up to date. This greatly facilitated legal compliance supervision in WP7. It is also worth noting that, even in the first iteration, piloting was done between the Netherlands and Romania using real

data (real users, and real evidences). To mitigate the legal risks, and in accordance with the terms of the MoU, the **exchanged evidence was however isolated** in the data evaluator systems, and could not be used for real life procedures. As a result, no legal impacts or risks could occur for pilot participants. This was manageable due to the relatively small number of pilot participants (less than ten, at the time of completion of this deliverable).

As an additional good practice, pilot usage was **recorded** as project data, but all personal and company data was **pseudonymized** prior to storage. As a result, the logs are usable for evaluation purposes, but cannot be used trivially to identify pilot participants. This follows the data minimization and data protection by design principles from the GDPR.

The pilot also faces the legal challenge of powers validation. Currently, it can rely on general powers of representation, which are verifiable based on eIDAS identification procedures. However, these are not fine-grained, since there are no EU ontologies of representation powers: it can be determined whether a natural person has a competence to represent a legal entity, but there is no way to automatically evaluate what this competence entails, and particularly whether it is appropriate for a specific use case (or for a specific SDGR procedure). To address this problem, the pilot is developing a **standardized powers catalogue**, tailored to the SDGR.

Assuming that the test results are positive, the catalogue still requires validation and formalization at the EU level, in order to give it legal authority (as opposed to its current *de facto* authority of being accepted by pilot participants as an approach purely for piloting and assessment purposes, which is the maximum DE4A can achieve). The necessary legal mechanisms to formalize the work exist, though, since the IR to the SDGR explicitly affirmed in recital (21) that "*The mutual recognition of national electronic identification means under [the eIDAS] Regulation applies to these cases of representation. [The SDGR] should therefore rely on [the eIDAS Regulation], and any implementing acts adopted on its basis, for the identification of users in cases of representation. The gateway coordination group and its subgroups should cooperate closely with the governance structures established under [the eIDAS Regulation] to help develop solutions for powers of representation and mandates.*" Thus, the outputs of this pilot stream could be escalated to these groups for validation and formal endorsement.

At a more practical level, this piloting stream also collected feedback from users on their experiences. Some criticism was levelled by the users at the standardised request/preview language created by WP7, which was seen as legally sound, but hard to understand and unappealing to read.

#### 3.3.1.3 Planned WP7 actions, notably in relation to the second iteration

In this particular pilot stream, thus far the Intermediation Pattern has been piloted, with the Subscription and Notification Pattern piloting expected to initiate in the coming months. This will require a reworking of the standardised request/preview language and possibly of the privacy notices, since the users must be made aware that exchanges may occur for some period of time after they have consented to it (even without a new individual request and preview for each subsequent exchange).

Moreover, the implementation and further testing of fine-grained powers validation will require further legal analysis to examine how the findings can be formalised. From a legal compliance, this should not trigger significant new concerns since the procedures will remain simulated here as well (i.e. the users and data are real, but the procedures are not, so that no real life consequences can occur).

### 3.3.2 Moving abroad

#### 3.3.2.1 Summary of pilot specificities

This stream targets individual citizens exercising their personal mobility rights, comprising three use cases:

| SDGR Procedure | DE4A Moving Abroad pilot use case |
|---|---|
| Registering change of address | Registering a change of domicile address |
| Citizens' and family rights | Requesting civil status certificates |
| Requesting information on the data related to pension from compulsory schemes | Requesting information on the data related to Career overview, pension simulation and claiming pension and pre-retirement benefits |

Table 3: Use cases in the Moving Abroad pilot

All of these apply the standard User-supported Intermediation Pattern. Five Member States are involved: Romania, Portugal, Spain, Luxembourg and Slovenia. At the time of submission of this deliverable, Spain is active as a data requester and Luxembourg is scheduled to follow in the coming weeks; and Spain, Slovenia and Portugal as data providers.

The principal challenges are to ensure the lawfulness of the exchange, taking into account national legislation, and the scoping of the users (i.e. the question of whether users can only be legally competent adults representing themselves, or also less common use cases of e.g. minors, or persons representing their entire family.

#### 3.3.2.2 Specific actions undertaken and lessons learned

Given the potential impacts on real life persons, currently piloting occurs only at the technical demonstrator level, with **fake data/fake persons only**. For that reason, risks to individual persons are virtually non-existent, following the risk categorisation of the MoU, and no specific safeguard measures were needed.

Following extensive scoping discussions, the decision was made to **focus only on cases involving a single legally competent and adult person, acting on behalf of themselves** (thus eliminating the concerns relating to the protection of minors, or validating powers of representation, including also parental authority as defined under national laws). From a legal perspective, this was necessary because there is no commonly accepted EU level legal model for determining and validating such powers. National systems exist to determine powers of representation (building e.g. on concepts such as parental authority, legal guardianship etc), but there is no automatic way to determine the legal value and meaning of these concepts, or their equivalence to similar concepts in other Member States. There were also other and more operational concerns, such as the need to integrate further interactions with the represented parties.

An additional lesson that was learned is the role and **impact of national legislation**. Portuguese law was found to contain a deregistration requirement as well: once a user changed their address to another Member State, it was mandatory to deregister that person from their Portuguese address. Other Member States are likely to have the same requirement, to avoid persons holding multiple official domiciles. This obligation required a modification in the standardised legal descriptions of the pilots (the privacy policy and disclaimers). Admittedly the actual legal impact of these modifications is very limited while piloting involves only fake persons/fake data.

#### 3.3.2.3 Planned WP7 actions, notably in relation to the second iteration

Up to the submission of this deliverable, the pilot stream has focused on the first use case only (request change of address), although the same approach and the same findings are also applicable to the second use case (request extract of civil certificate).

In the second iteration, piloting with real users will occur in Q4 2022 and Q1 2023; this will require an update of the disclaimer, privacy policy, and the MoU compliance table. Representation cases may

then occur as well, although this will require a further legal analysis of the conditions under which this may be done.

### 3.3.3 Studying abroad

#### 3.3.3.1 Summary of pilot specificities

This stream targets students in particular, and comprises three use cases:

| SDGR Procedure | DE4A Studying Abroad pilot use case |
|---|---|
| Applying for a tertiary education study financing, such as study grants and loans from a public body or institution | Use case 2: Applying for study grant |
| Submitting an initial application for admission to public tertiary education institution | Use case 1: Application to public higher education |
| Requesting academic recognition of diplomas, certificates or other proof of studies or courses | Use case 3: Diploma recognition |

Table 4 : Use cases in the Studying abroad pilot

Three Member States (Spain, Portugal and Slovenia) are involved, and the use cases apply both the standard User-supported Intermediation Pattern, and the Verifiable Credentials Pattern. At the time of submission of this deliverable, all three Member States have data providers and data requesters running in at least one use case. Piloting was done with real persons (students) in coached/guided testing sessions, and some real data was used. The procedures were however fake, in the sense that no real life consequences were attached to them (corresponding to medium risk testing in the MoU risk categorization).

The unique elements of the pilot stream are the direct involvement of universities as pilot partners (who are not normally direct users of eIDAS nodes and eDelivery Access Points), and the use of the Verifiable Credentials Pattern.

#### 3.3.3.2 Specific actions undertaken and lessons learned

This workstream made **good use of the provided legal compliance templates**, which were kept up to date. Similar to the Doing Business Abroad pilot, piloting used real data (real users, and real evidences) in some instances, but **exchanged evidence was not used for real life procedures**. As a result, no legal impacts or risks could occur for pilot participants.
As a good practice, it can be highlighted that this pilot stream queried the student participants on their experiences and impressions. For the legal lessons learned, it is intriguing to note that the pilot participants **appreciated the clarity of the explicit request and preview interfaces**, which they experienced as an approach that highlighted and enabled their control over their own data (in contrast to the DBA pilots, where the professional use found them unappealing and complex). Possibly, the direct interaction during testing sessions was the key differentiating factor.

For the VC pattern, interactions with **EBSI** were organized and supported by WP7, so that the credentials could build on the DLT infrastructure in the EU. This was relatively straight forward, since the agreements were fairly light and accessible, but still required some coordination to ensure that all pilot participants interpreted and completed the agreements in the same way. Furthermore, given the requirements of the GDPR, the **blockchain was only used to support and store non-personal data**, as no clear legal basis seemed available to justify different choices.

Finally, the VC documents issued during piloting have no formal legal value, reducing the possibility of using them in real procedures: while the underlying academic data is real, **the actual VC generated and used during piloting is anonymized,** for data protection reasons (i.e. to avoid real data being made available to a third party who has no legal justification to use it). This can be considered a good practice, since it allows realistic testing to occur without exposing the data to third parties.

#### 3.3.3.3 Planned WP7 actions, notably in relation to the second iteration

While piloting will be further expanded, an extension to real procedures with real legal consequences is not planned. This is for practical reasons: the student registration period in real procedures does not overlap with the piloting period. None the less, legal challenges will continue to be monitored until the conclusion of piloting.

# 4 Conclusions

## 4.1 Principal observations and lessons learned

As the preceding sections will have shown, significant work has been done to support legal and ethical compliance of the DE4A project in general, and of piloting in particular. These relate both to more routine outputs (such as privacy policies and disclaimers), and to more complex and detailed outcomes (such as the wireframe guidance, Memorandum of Understanding and the monitoring templates).

Generally, piloting has been relatively successful thus far, with the following caveats:

- Creating sufficient **transparency** with respect to the piloting activities remains difficult. The information obligations in the SDGR and the IR are quite detailed and demanding, and moreover they must often be combined with data protection transparency obligations under the GDPR. This can result in lengthy interfaces, with multiple steps to be completed, and relatively detailed legal information in separate policy texts. This approach has received a mixed response, with some users commenting positively on the notifications and interfaces, and others indicating that they needlessly added effort and slowed the process down. The extensive transparency obligations defined under the SDGR and GDPR must be complied with, but it is worth examining how they can be streamlined.
- Effective **monitoring** has been important to keep track of legal compliance. The DE4A project chose a pragmatic approach, in which the piloting partners had to keep track of the piloting status, report on this via lightweight standardised templates, which were verified by WP7, including the DE4A data protection officer. No compliance incidents were logged, which may have been partially aided by the summaries of legal obligations via the standardised templates.
- Piloting in **real life procedures with real data and real users** obviously creates additional legal compliance concerns, which are hard and sometimes impossible to mitigate for some use cases. As the SDGR has not yet entered into complete application, this raises doubts on the extent to which exchanges can already take place in real life procedures. This is however an inevitable part of piloting prior to the entry into application of the legal framework.
- While the SDGR framework is now relatively completed (through the adoption and publication of its IR), there are a very high number of **legal dependencies with other frameworks** that have not been comprehensively resolved. The revision of the eIDAS Regulation (which could significantly support the use of verifiable credentials as piloted in DE4A) is still underway; and the critical topics of company representation and identity matching have not been conclusively settled yet. DE4A provides good practical experiences on these topics that can be built on, but these still require adoption and endorsement at the EU level outside of the project.
- Finally, it is also worth underlining that the SDGR/IR focus on **one particular way of implementing once-only,** namely by making the users the gatekeepers of evidence exchanges relating to them, and emphasizing data exchanges between competent authorities. Other perspectives are possible, as shown in the subscription/notification pattern (that could also be used to strengthen once-only exchanges in a way that serves both the public and the individual interest), and as shown in the ongoing eIDAS 2 discussions surrounding notably mobile identity wallets (which would strengthen the user's position as a holder of their data, rather than just the gatekeeper of exchanges). Since the SDGR does not focus on these other perspectives, reflection is needed on whether these perspectives should become a part of the European once-only policy and legal framework, and how they can then be integrated.

## 4.2 Planned further actions in DE4A

It is also clear that significant work still lies ahead. The ambitions of the individual pilots in the second iterations are clear, and this will require:

- **Continued monitoring** of the piloting actions, especially where the risk qualification changes (e.g. as a result of a shift from fake users/data/ procedures to real ones), or where new use cases go live and new interaction patterns are integrated.
- **Continuous updates to the legal/ethics texts**, such as the privacy policies, disclaimers, and the DPIA**,** to ensure that they continue to reflect the reality.
- **Evaluation of the transparency approach** to improve readability and accessibility.
- **Monitoring of legislative changes,** notably in the context of the ongoing eIDAS 2 discussions.
- **And assessing the legal challenges relating to the more legally complex patterns, notably the Subscription and Notification pattern and the Verifiable Credentials pattern,** to ensure that these remain within the boundaries of the law as well.

## 4.3 Initial recommendations on future actions outside of DE4A

Finally, the overview above also shows that there are some topics for which DE4A can (and does) define and pilot solutions, but external action will be necessary to ensure that these solutions are supported both by policy and legislation. This refers in particular to:

- The **representation of legal entities,** for which a pragmatic ontology has been created in DE4A that needs to be extended, validated and formalised in the context of the eIDAS Regulation;
- In the longer term, possibly also the **representation of natural persons** (such as parents representing their children) will require a more structural solution.
- Discussions surrounding **an extended perspective on once-only exchanges** must be held**,** such as cases where data can be exchanged in the longer term without seeking new prior requests and previews, or even exchanging data in well defined cases of public interest (e.g. to combat fraud, detect errors, or proactively grant benefits) even when there has never been a request from the user. This will be important to settle the notification and subscription patterns.
- The **eIDAS 2 revision needs to be finalised**, and the interaction between **mobile identity wallets and once-only exchanges must be clarified.** It is clear that the identity wallets foreseen under the eIDAS 2 proposal will be perfectly usable for identification and signing functionalities in SDGR procedures, but it is less clear that making evidence available to the user and allowing them to share it with competent authorities would be considered a once-only exchange under the SDGR. In relation to that, the link between **verifiable credentials and the eIDAS 2 concept of an "electronic attestation of attributes**" should be clarified: if verifiable credentials can be issued as qualified electronic attestations of attributes that can be validated through authentic sources (as foreseen under the eIDAS 2 proposal), then this would resolve some of the current discussions on the legal validity, value and verifiability of such credentials.

DE4A will of course contribute to these discussions, by making its findings and analysis available, and disseminating its knowledge, especially via partners participating in EU level expert groups and cooperation groups.

# 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, D10.2 POPD Requirement n°2 (2020)

[13] 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

[14] 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

[15] 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

[16] DE4A Consortium, D7.1 Overview of legal and ethical requirements (2020).

[17] DE4A Consortium, D7.2 Initial Report on legal and ethical recommendations and best practices (2022).