D7.2 Initial Report on legal and ethical recommendations and best practices

Document Identification			
Status	Final	Due Date	31/12/2021
Version	1.2	Submission Date	26/01/2022

Related WP	WP7	Document Reference	D7.2
Related Deliverable(s)	WP4, WP7, WP8, WP9	Dissemination Level (*)	PU
Lead Participant	Timelex	Lead Author	Hans Graux, Mahault Piéchaud Boura (Timelex)
Contributors	Hans Graux, Mahault Piéchaud Boura (Timelex)	Reviewers	Ard van der Heijden (RVO) Gérard Soisson (CTIE)

Keywords :
Ethics, legal, requirements, compliance, SDGR, GDPR

Disclaimer
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
Mahault Piéchaud Boura	Timelex

Document History			
Version	Date	Change editors	Changes
0.1	31/08/2021	Hans Graux	Initial version of document
0.5	15/11/2021	Mahault Piéchaud Boura	First round of updates; drafting first open discussion points
0.7	15/12/2021	Hans Graux	Integration of best practice inputs (sample texts, DPIA, comments)
0.9	11/01/2022	Hans Graux	Finalisation for internal validation
1.0	19/01/2022	Hans Graux	Integration of feedback from Ard van der Heijden (RVO)
1.1	23/01/2022	Hans Graux	Final version for submission; integration of feedback from Gérard Soisson (CTIE)
1.2-1.3	24/01/2022	Atos	Final check and update for submission

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Hans Graux (Timelex)	23/01/2022
Quality manager	Julia Wells (ATOS)	24/01/2022
Project Coordinator	Ana Piñuela Marcos (ATOS)	24/01/2022

Table of Contents

List of Tables

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
CPSV	Core Public Service Vocabulary Application Profile
DCAT	Data Catalog Vocabulary
DE4A	Digital Europe for All (this project)
DEP	Digital Europe Programme
DPIA	Data Protection Impact Assessment
DSM	Digital Single Market
EESSI	Electronic Exchange of Social Security Information
EIF	European Interoperability Framework
EIRA	European Interoperability Reference Architecture
EU-GIP	EUropean Governmental Interoperability Platform
GDPR	General Data Protection Regulation
ISA2	Interoperability solutions for public administrations, businesses and citizens
LSP	Large Scale Pilot
MoU	Memorandum of Understanding
N/A	Not Applicable
NRT	Near Real Time
OOP	Once Only Principle
OSI	Open Systems Interconnection model (OSI model)
PSA	Project Start Architecture
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/

Abbreviation / acronym	Description
ZKP	Zero Knowledge Proof

Executive Summary

This deliverable is the second formal output of WP7 (Legal and ethical compliance and consensus building) for the DE4A project and aims to summarise all legal and ethical compliance activities undertaken in the course of the project, including any recommendations, draft texts, and legal and ethical best practices that were agreed between DE4A participants for the purposes of the project.

As will be highlighted at several points throughout this document, it does not aim to capture conclusive findings on all legal and ethics topics. A central goal of WP7 and of DE4A in general is to move towards a consensus on best practices around the operationalisation of abstract legal requirements formulated in the SDGR. Discussions are still ongoing between Member States, and towards the European Commission, on the exact interpretation and intended impact of the SDGR. Moreover, the legal framework is not yet entirely complete, as will be commented below, which creates some uncertainties.

None the less, this report aims to present the central topics that have been under discussion within the consortium, and captures the main efforts undertaken to adhere to the terms of the SDGR and other legislation at the time of submission, and to satisfy ethical requirements, including but not limited to data protection.

The report comprises two major sections:

- Firstly, it summarises 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.
- Secondly, it contains a summary and prospective discussion of legal and ethical topics for future policy reflection. This is an initial description of areas where new legal or ethical reflection may need to occur in the future, since some of the experiences in DE4A exceed the current legal vision of the SDGR. The future discussion topics do not contain a consensus position from the entire consortium on desired outcomes, but rather aim to signal points where there is legal or ethical margin for evolution in the future.

The contents of this report were developed iteratively and interactively through discussions between all project partners and will be maintained and revised until the end of the project (as is foreseen in the Grant Agreement, since this D7.2 is expected to be updated into a final and conclusive D7.3 - Final Report on legal and ethical recommendations and best practices), due in the last months of the project. Therefore, the positions taken in this deliverable may not necessarily be conclusive, but they are informed and driven by existing understanding of the law and ethics across DE4A members.

1 Introduction

1.1 Purpose of the document

The present document is the second 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.

In addition, this WP aims to formalise a 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 second deliverable in WP7, summarises all legal and ethical compliance activities undertaken in the course of the project, including any recommendations, draft texts, and legal. These result 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).

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 its main findings and points of attention will be included below, to facilitate an assessment of why certain legal and ethical compliance issues were undertaken.

Since the objective of this document is to report on legal and ethical actions undertaken in the course of DE4A, a specific section will be included that reports some of the major practical outcomes, including sample legal texts and disclaimers, the Memorandum of Understanding, and the Data Protection Impact Assessment.

However, a key challenge for WP7 – and for DE4A as a whole – is the current 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 – a so-called Implementing Act – by 12 June 2021, to set out the technical and operational specifications of the technical system. While significant advances were made and an advanced draft proposal was established (but not yet made publicly available), the Commission ultimately has not been able to meet this deadline, and at the time of submission of the present deliverable, no finalised Implementing Act is available. Significant and mature analysis can be done on the basis of the draft proposal, but until a final Act is adopted, uncertainty remains.

Secondly, 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 e-government services in general. Alternatives to the perspective of the SDGR can be considered, and as will be commented below, DE4A also aims to do so by exploring alternative evidence exchange patterns. These raise new legal and ethical concerns and opportunities, which also should be addressed, since they may feed into future EU or national level policies. For that reason, this report also contains a more prospective section, which provides an initial and high level perspective on the legal and ethical implications of these alternative perspectives, thereby providing a more advanced understanding of potential new evolutions, and how these can be managed from a legal and ethical perspective.

As foreseen in the Grant Agreement, the current document is a snapshot of outputs and interpretations in DE4A at the time of submission. Both the concrete outputs and the legal and ethical assessments are highly subject to evolution and will be updated to reflect pilot experiences and discussions between the Member States and the European Commission on the implications of the SDGR and its further implementation. As a result, D7.2 should be seen as a living document, which will be maintained and expanded in the course of the project, and for which current positions will be revised as the project's understanding of the SDGR and once-only matures.

1.2 Structure of the document

This document is divided into five main sections:

- Chapter 2 – General outline of the legal and ethical requirements of the SDGR. 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.
- Chapter 3 – Summary of legal issues. This is a short summary of the main legal issues as identified and described in detail in D7.1 - Overview of legal and ethical requirements. The objective is to ensure a clearer understanding of the legal and ethical framework within which DE4A operates
- Chapter 4 – Legal and ethical actions undertaken. This chapter describes the measures already undertaken in DE4A, including both actual sample texts provided, and the reasoning behind the texts.
- Chapter 5 – Topics for future reflection. This chapter highlights some of the main legal and ethical open discussion points, i.e. situations where the current legal and ethical framework is not ideally suited yet to some of the once-only concepts that could benefit European e-government.
- Charter 6 – Conclusions. This chapter outlines the main findings and lists next steps in WP7.
- Annex I – DE4A DPIA. This chapter presents the DPIA that has been drafted to assess data protection risks within the DE4A project, with the objective of mitigating them as far as possible, in accordance with the requirements of the General Data Protection Regulation.
- Annex II – DE4A MoU. This chapter describes the MoU, drafted to support the piloting activities between partners and/or their direct and indirect agents.

2 General outline of the legal and ethical requirements set in the SDGR

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 first chapter of the deliverable briefly describes the requirements of the SDGR, and more importantly explains why and to what extent the SDGR is not the only driver for legal and ethical requirements.

2.1 The SDGR's 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;

[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.

- 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[5]. 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, 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,

[5] As a simple point of practicality, piloting initiatives in DE4A only aim to test the implementations of the once-only principle and are not representative of final e-government services; therefore the pilot services are offered as digital-only and once-only by default.

the SDGR relies on the legal framework of the eIDAS Regulation, which causes some practical and legal challenges, as will be explored in Section 5.2.3 below.

2.2 Requirements for the technical system under 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. The next chapter will examine the more challenging requirements in greater detail.

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. For that reason, the requirements established by Article 14 of the SDGR 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. 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 requirements.

A key example is the case of proactive, automated or recurring evidence exchanges, which are not individually driven by a new request and a new preview for each individual exchange. These 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 to some extent, but as will be explained below, specific safeguards and constraints are implemented to ensure that evidence is not exchanged without a prior request. 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: 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 examples can be valuable, but 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, the DE4A project aims to pilot at least some of these patterns in the future, 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.

3 Summary of legal issues in DE4A

Task 7.1 in DE4A aims to identify and scope the legal and ethical requirements for the development of the DE4A solution and the execution of the pilots. Relevant requirements have been identified based on the analysis of the SDGR, GDPR, and in discussion with the partners; and they have been reported upon in D7.1 - Overview of legal and ethical requirements. For a full review of relevant requirements, we refer to that deliverable.

In this specific Chapter, a brief summary will be provided of the main issues commented upon in D7.1. The reason is practical: since the main objective of this report is to comment on legal and ethical achievements in DE4A, it is important to first identify the questions that were taken into consideration when implementing legal and ethical actions.

Within D7.1, seven topics were discussed at some length:

- The preview requirement of the SDGR
- The explicit request requirement of the SDGR
- GDPR data subject rights in relation to once-only exchanges
- Requirements on the structure of exchanged evidences
- Charging and costs for evidence exchanges
- Further processing of evidences by competent authorities after the exchange
- And the lawfulness and legal basis of piloting activities.

Each of these topics will be described below, along with a short summary of the relevant actions required during DE4A (if any). For more detailed analysis, we refer to D7.1.

3.1 Preview of evidence exchanged

3.1.1 Description of the requirement

According to the Single Digital Gateway Regulation, the envisaged technical system "*shall enable the possibility for the user to preview the evidence to be used by the requesting competent authority and to choose whether or not to proceed with the exchange of evidence*" (14.3 (f) SDGR).

The technical system for the cross-border exchange of evidence must thus support a mechanism of preview by the user of the evidence, and a mechanism of approval of the exchange after observing the preview (thus also preventing the exchange by refusing to approve it). However, the wording of the preview mechanism in the SDGR clearly indicates that the preview is only a *possibility* that must be afforded to the user, not that the user has to be required to actually use (observe) the preview. Exceptions to the general rule exist, as will be explained below.

The SDGR does not state explicitly when the preview should take place; it merely notes that the technical system should "enable the possibility for the user to preview the evidence to be used by the requesting competent authority and to choose whether or not to proceed with the exchange of evidence". The D7.1 argued that the preview should occur with the data providing Member State, or alternatively with the Data Requestor, for data protection reasons. It noted also that the Data Requestor role might be more viable in practice, since organising the preview at each individual data provider implies complex data flows. After the submission of that deliverable, a draft Implementing Act was published that noted that the portal website of the evidence requester should provide a preview space, from which data is deleted after the preview – which is therefore different from what was originally envisaged in D7.1 (which favoured previews with the Requestor, but not with the Evaluator).

3.1.2 Relevance and required actions

The preview requirement is a legal and ethical safeguard under the SDGR, and therefore is applied in DE4A as well. Moreover, even in exchange patterns that would not be direct implementations of the SDGR, the preview requirement should be retained and implemented, since this is a direct safeguard that was chosen by the European legislation in cross border once-only transactions that protects the users against unlawful data exchanges.

The main implication is that the preview functionality had to be implemented, and from a legal perspective relevant notices were needed to communicate to users that they had the right and ability to preview relevant exchanges, prior to deciding whether to permit an exchange.

However, it is worth noting that DE4A does not always implement the preview functionality at the site of the evidence requester, as the draft Implementing Act would require, since that would result both in technological complexity and arguably greater privacy and security challenges: if the evidence requester has to provide the preview, that means they already requested and received the evidence from the evidence provider. An exchange therefore has already occurred, prior to the preview. For that reason, DE4A allows evidence to be previewed at the evidence provider's infrastructure as well. This achieves a higher level of protection and greater ease of implementation, and is not currently legally problematic since it is not contrary to the SDGR: only the draft (and therefore not approved) Implementing Act states a preference for requester-side previews; the SDGR does not do this, as is explained in more detail in D7.1. No evidence is used in a procedure until the request has been made by the user, of course, irrespective of where the preview is organised. Moreover, as will be explored in more detail below, not all procedures are in scope of the SDGR, and therefore not all procedures would be bound by a final implementing act.

3.2 Explicit request

3.2.1 Description of the requirement

According to the SDGR, the envisaged technical system "*shall enable the processing of requests for evidence at the explicit request of the user*" (14.3 (a) SDGR). Moreover, it adds that the "*use of the technical system shall not be obligatory for users and shall only be permitted at their explicit request, unless otherwise provided under Union or national law*" (14.4 SDGR).

Requirements for the validity of such an explicit request are also outlined in the SDGR, which stresses that it must be "*an explicit, freely given, specific, informed and unambiguous request of the user concerned*", as a result of which consuming authorities must "*request evidence directly from competent authorities issuing evidence in other Member States through the technical system*" (article 14.7 SDGR). The technical system for the cross-border exchange of evidence must thus support a mechanism for the user to express an explicit request that meets the requirements above.

Article 14 thus takes a very user-centric perspective, in the sense that the exchange must in principle be driven by a user request. This puts the user in control over the evidence exchange, which has both benefits and downsides. The benefit – and objective – is that the user is protected against potentially unlawful exchanges of evidences without their knowledge. The downside is that the user must in principle be involved in authorising an exchange. As recital (44) phrases it, the SDGR "*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*".

A transfer that would be beneficial for competent authorities (or for the public interest) may be defensible from a public policy perspective even without the request (or even knowledge) of the user, and it can even be considered an application of a broader interpretation of the once-only principle, but the SDGR does not allow such exchanges in principle – subject to the exceptions discussed below.

3.2.2 Relevance and required actions

The SDGR indicates that the "*use of the technical system […] shall only be permitted at their explicit request, unless otherwise provided under Union or national law*". This would suggest that the explicit request must occur prior to using the technical system. Since user interactions are initiated at the data consumer's side, it should be the data requesting authority that collects the explicit request. This is the position that was taken in D7.1, and which was also affirmed afterwards in the draft Implementing Act.

The implication is that the explicit request functionality had to be implemented, and from legal perspective relevant notices were needed to communicate to users what they were requesting. An additional complexity created by the draft Implementing Act is that it specified which information had to be provided to users when requesting evidence exchanges, including notably an explicit identification of the name of the evidence issuer and a name of the evidence type; as well as the option to select which evidences to exchange or not. The legal notices had to reflect these points.

Additionally, as was already described above, DE4A also supports a lookup function that allows an authority to consult publicly available information without a prior request; but since this information is publicly available, it is exempt from the prior request requirement. Similarly, the subscription and notification pattern only exchanges information that indicates whether evidence has changed; since no actual evidence exchange occurs, no prior request is therefore required.

3.3 Data protection and data subject rights in the context of the SDGR

3.3.1 Description of the requirement

One of the main objectives of the GDPR was to establish a set of data subject rights, which are available in any situation where personal data is being processed, across the EU, regardless of where the data is processed. These rights are set out in Chapter III of the GDPR, and include the rights to[6]:

- obtain information about the processing of your personal data;
- obtain access to the personal data held about you;
- ask for incorrect, inaccurate or incomplete personal data to be corrected;
- request that personal data be erased when it's no longer needed or if processing it is unlawful;
- object to the processing of your personal data for marketing purposes or on grounds relating to your particular situation;
- request the restriction of the processing of your personal data in specific cases;
- receive your personal data in a machine-readable format and send it to another controller ('data portability');
- request that decisions based on automated processing concerning you or significantly affecting you and based on your personal data are made by natural persons, not only by computers. You also have the right in this case to express your point of view and to contest the decision.

The exchange of evidence in the context of the SDGR usually implies the processing of personal data – occasionally because the evidences contain personal data, and structurally because the exchange includes at least metadata in relation to a physical person who has triggered the exchange. As a result, the exercise of the aforementioned rights should be possible in the context of the SDGR as well.

Therefore, it is the duty of the competent authorities to support data subject rights in relation to their procedures, in the same way and to the same extent that they have already been required to do so prior to the SDGR. The SDGR does not introduce new data subject rights and does not limit or expand data subject rights that are already available under the GDPR.

[6] See https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/what-are-my-rights_en

3.3.2 Relevance and required actions

In the context of the SGDR and the technical system, there is no legal obligation to develop specific functionalities or components to support the exercise of data subject rights. However, to ensure that citizens have a way to exercise their data subject rights, the relevant data protection policies / privacy policies had to be created, including identification of the relevant participants in any given pilot, and a specific point of contact where more information could be obtained, or where other rights requests could be exercised. This is of course also applicable in cases where the exchange patterns do not align directly with the SDGR's perspective on the OOP, since data subject rights are dictated by the GDPR, rather than the SDGR.

Moreover, DE4A relies on regulated electronic identities, specifically identities that were notified at the EU level in accordance with the requirements of the eIDAS Regulation, so that it relies on legally trustworthy identity information. This is a requirement under the SDGR, but obviously also helps to mitigate data protection concerns, since it increases the quality and trustworthiness of exchanged personal data, and reduces the chances of identity fraud (and any resulting untrustworthy exchanges of evidence). Thus, while the use of eIDAS identities is not a pure GDPR compliance choice, it does have clear data protection benefits, and makes it less likely that data subjects will need to avail themselves of their data subject rights to rectify problems.

3.4 Structured and unstructured evidence in the context of the SDGR, and proportionality

3.4.1 Description of the requirement

The SDGR's provisions in relation to the once-only principle (Article 14) aim to ensure that certain types of evidence can be exchanged via the technical system, in the procedures falling within the scope of the Regulation. More specifically, Article 14.2 of the SDGR notes that "2. Where competent authorities lawfully issue, in their own Member State and **in an electronic format that allows automated exchange**, evidence that is relevant for the online procedures referred to in paragraph 1, they shall also make **such evidence** available to requesting competent authorities from other Member States **in an electronic format that allows automated exchange**" (emphasis added).

Therefore, the only evidences that must be made available for exchange within the scope of the SDGR are those which are issued "in an electronic format that allows automated exchange". If such evidences are available, they must also be made available in the same format.

This raises a key issue: when exactly can evidence be considered to be "in an electronic format that allows automated exchange"? More specifically, does this description imply that the evidence must be formatted in a semantically meaningful way – i.e. must it be structured in a way that allows the evidence to also be interpreted and processed automatically, at least to some extent, by the receiving competent authority? Or from the opposite perspective: does it imply that unstructured evidence, such as a graphic image (a bitmap, JPEG, or PDF scan without a semantic structure), should not be considered to be evidence falling within the scope of Article 14?

In D7.1, the perspective was taken that the SDGR does not mean to introduce any possibility to discriminate between structured and unstructured evidences, and therefore that both types of evidences must be supported. This interpretation was thereafter also confirmed by the Commission.

As a matter of practicality though, within DE4A electronic evidence can be shared either as the original evidence (without any modification of any kind), or also include the so-called canonical evidence (a standardised and structured form of the evidence, that however aims to introduce no substantive changes to the content of the evidence). This too was supported by D7.1, which argued that the addition of such data would be permissible to enable automatic processing. Legally speaking, only the original (unmodified) evidence is evidence in the sense of the SDGR; the canonical evidence is produced only to allow further automatic processing.

This also triggered questions around the exact scope of the preview functionality. The SDGR generally requires that the user must have the possibility to preview the evidence prior to the exchange. If both original and canonical evidence is exchanged, it is relevant to assess whether only one of these or both must be available for preview. Since the original evidence is the authentic evidence, at a minimum that should be available for previewing. However, in reality, further processing after the exchange is likely to be driven by the contents of the canonical evidence, which should be – but is not guaranteed to be – identical to that of the original evidence. This is a problem that in theory should not occur, since only the original evidence has legal authority, but in practice may occur, especially if and when canonical evidences become seen as being accurate and trustworthy. To mitigate this risk, both should be available for preview to the user.

Related to this, there was also the question of proportionality. Article 14.8 of the SDGR contains a data minimisation principle (comparable to the same principle under the GDPR), noting that "*The evidence made available to the requesting competent authority shall be limited to what has been requested and shall only be used by that authority for the purpose of the procedure for which the evidence was exchanged*". This raised the question of whether there was any obligation to filter evidences provided, by omitting data from the evidences that would not be relevant to the procedure. It was agreed that such filtering was neither formally required by the SDGR, nor practically feasible, since this would require extensive micromanagement at the procedural level: each procedure would not only have to identify which evidence type would be required, but also which data from that evidence would be necessary, and what would need to be omitted. Therefore, minimisation is only applied to evidence types, not data fields.

3.4.2 Relevance and required actions

The principal legal and ethical obligation is to identify during the evidence request stage exactly which evidence will be exchanged. Moreover, if canonical evidence is also exchanged, this must be visible as well. While this is not legally required by the SDGR (which does not contain the concept of canonical evidence), this is required to reduce risks, and to include appropriate ethical safeguards that support good administration. If canonical evidence is included, the likelihood is after all that this evidence will be used by the receiving administrations – who should, in theory, verify it against the original evidence, since on this original evidence has legal value. However, there is a conceptual risk that this will not occur in practice. For that reason, it is advisable that the canonical evidence should be subject to at least the same level of potential scrutiny by the user as the original evidence under the SDGR. This is an example of a variation on the SDGR introduced by DE4A that increases utility, and which also results in the need for an additional legal and ethical safeguard (namely transparency and preview rights for the canonical evidence as well).

3.5 Charging for evidences under the SDGR

3.5.1 Description of the requirement

A recurring topic of discussion is the issue of charging for evidence. In SDGR procedures, it is possible that a user has to pay to obtain certain evidences from an issuing authority. By way of examples, an extract from a business register may not be free, or even a birth certificate could in theory require a charge covering the administrative cost born by the authority. The SDGR does not affect this ability to charge. Therefore, the consensus position in DE4A is that there is no formal legal obligation for Member States or their authorities to modify or eliminate their charging policies in the context of the SDGR. In other words, if the issuing competent authority already charges a fee to the user for evidences outside of the context of the SDGR, they can also do so for procedures covered by the SDGR.

3.5.2 Relevance and required actions

Given that the payment issue is considered as an external problem that does not require a specific solution to be developed in DE4A, no action is required. Moreover, none of the planned pilots imply a payment to be made.

3.6 Further processing of evidences

3.6.1 Description of the requirement

The central question here is whether, once a data consuming authority has received evidence in accordance with the SDGR, they can share it with additional authorities within their own country. The position established by D7.1 was that the SDGR governs only the exchange of evidences in the procedures listed in the SDGR; but once that transfer has occurred and the data consuming authority has received their evidence, any further use of the evidence is governed only by national law as applicable to the receiving competent authority. It is likely that some Member States will have their own once-only principles, governed by national laws, under which they share data with other public administrations, or under which they are required to retain evidences after receiving them under the SDGR. There seems to be no prima facie reason why the SDGR would invalidate such national laws. Therefore, such further use would remain lawful.

3.6.2 Relevance and required actions

Since further use is governed by national laws, the principal requirement is that this interpretation (and thus the possibility of further use under national law) is clearly disclosed to the user through DE4A's standard interfaces.

3.7 Lawfulness / legal basis of piloting prior to the entry into application of the SDGR

3.7.1 Description of the requirement

A horizontal concern for all piloting activities is the existence of a legal basis for the exchange of evidences between competent authorities for the duration of DE4A. The principal challenge is that Article 14 of the SDGR largely becomes applicable only as of 12 December 2023, as set out in Article 39 of the SDGR, whereas piloting will start much sooner. This raises challenges on the legal basis for any exchanges of real life evidences relating to real life citizens and businesses (as opposed to mock fictitious data, for which no such legal basis would be needed). This point is especially salient in relation to evidences containing personal data, since any processing of personal data requires a clear legal basis under the GDPR.

A partial solution is the interpretation that piloting activities have a lawful legal basis under article 14 of the SDGR, on the grounds that the SDGR has been adopted and will become effective at the end of 2023, and that specifically article 14.11 of the SDGR has already entered into force, as stipulated in article 29 of the SDGR. Article 14.11 notes that "*The Commission and each of the Member States shall be responsible for the development, availability, maintenance, supervision, monitoring and security management of their respective parts of the technical system*". Development activities therefore already have an explicit legal basis, both for the Commission and for the Member States – which is reasonable and a prerequisite to allow the system to be created prior to becoming fully operational. It could be reasonably argued that piloting is a natural part of development activities, since development cannot be concluded without piloting tests; and that well scoped and limited piloting activities therefore also have a legal basis under the SDGR. Under that reasoning, piloting has a legal basis. From a data protection perspective, piloting can then be considered to be necessary for the performance of a task carried out in the public interest or in the exercise of official authority, as stipulated by Article

6.1 (e) of the GDPR (presuming of course that all constraints of the SDGR and GDPR are also complied with).

This perspective is however not universally endorsed by all Member States. Moreover, it only reasonably applies for piloting activities within the scope of the SGDR – i.e. for piloting activities covered by the Annexes or the included Directives – and only provided that the legal constraints of the SDGR are respected. If Member States choose to explore exchange patterns that fall outside of the limitations of the SDGR – which some of them will do, as will be further commented below - a separate legal basis would be needed, separate from the SDGR, in principle building on national laws (supported of course by the EU level requirement of complying with the GDPR, which is after all a transversal requirement).

3.7.2 Relevance and required actions

To mitigate these issues to some extent, it was agreed to further scope piloting activities through a Memorandum of Understanding, to be concluded between piloting partners, as was also done in prior Large Scale Pilot projects. This strengthens the legal basis underpinning piloting activities, at least for the duration of the project. In the longer term, other and more mature sustainability approaches need to be found, especially since some of the piloting of DE4A exceeds the scope of the SDGR. This legal sustainability topic is the core focus of a future deliverable (D7.4 - Report on legal sustainability).

4 Legal and ethical actions undertaken

Based on the analysis above and driven by feedback from pilot partners and Member States, a broad range of legal and ethical compliance activities were undertaken. These will be briefly summarised in this chapter.

4.1 Prior ethics activities under Work Package 10

DE4A project's ethics requirements are managed in detail within Work package 10 - Ethics Requirements. For that reason, some of the key ethical outputs can be found in separate deliverables, notably:

- D10.1 Requirement n°1 – Identification and recruitment of participants
- D10.2 Requirement n°2 – Data Protection Officer
- D10.3 POPD Requirement n°3 – Further processing

The principal contents of these deliverables are summarised hereunder.

4.1.1 Identifying and recruiting participants - information and consent scheme

Under the GDPR, any data controller – i.e. the entity that determines the purpose and the means of processing personal data - has a duty to inform data subjects of the processing of personal data concerning them. As a result, when piloting activities involve real natural persons (as opposed to using mock data or relating only to legal entities), they must be notified on the scope of processing as required by the GDPR. Therefore, several avenues for informing data subjects were implemented for the purposes of DE4A.

- A generic privacy policy and a cookies policy are freely accessible on the DE4A website to inform visitors of the processing of their personal data triggered by their visit of the website or when they contact the consortium.
- In relation to the pilots, D10.1 provided early guidelines and templates for the consortium members to inform data subjects of the scope of piloting activities and to obtain their consent, following the requirement of article 13 of the GDPR.

Deliverable D10.1 moreover addresses the procedures and criteria used to identify and recruit pilot users, the informed consent procedures to be applied, and provides templates to inform the pilot users. This work was provisional, and has been extensively revised in the meantime, as will be explained further below.

4.1.2 Appointment of a DPO

The DE4A consortium has appointed a Data Protection Officer[7] with suitable professional qualities. The DE4A DPO supervises the actions of the DE4A consortium to ensure they are complying with GDPR requirements for the processing of personal data, and provides advice where needed. For the avoidance of doubt, the DE4A DPO does not supervise the processing activities of the consortium members when they act in their capacity of public authorities for their mission at the purely national level outside of their piloting efforts of the DE4A project. The consortium members who are public authorities are required, under article 37.1 (a) of the GDPR, to appoint their own DPO, separate from the DE4A DPO.

The contact details of the DPO have been added to the privacy policy of the website, and are included in privacy statements pertaining to the pilots.

4.1.3 Further processing issues

The processing of personal data beyond the initial purpose for which it was collected is ‘further processing’ in the sense of the GDPR. In principle, further processing is not possible, as it is contrary to the principle of purpose limitation, which is a fundamental data protection principle according to which data is collected for specified, explicit and legitimate purposes.

There are however exceptions; mainly, further processing is admitted if the purpose is compatible with the purpose of the ‘primary ‘ processing, or when the data subject consented to the further processing, or even, when the processing is based on EU or national law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1). This issue has been described in some detail in D7.1, which argues that DE4A’s further processing is lawful, based on the safeguards provided.

4.2 Wireframes, disclaimers, and privacy policies

As was highlighted in the prior sections, 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;
- Two 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 usable for operational and non-operational piloting cases.

All of these required instantiation and customisation based on the individual pilots. Moreover, depending on the local context, live piloting would require translation to the local language(s). Microsites are maintained on a pilot stream basis, on which relevant disclaimers and privacy policies can be centrally maintained.

[7] See D10.2 POPD Requirement n°2

The templates are published online and maintained live via the DE4A legal wiki pages. Static versions are included below.

4.2.1 Standardised disclaimer for non-operational piloting

The services and applications provided as a part of this pilot have been set up in the context of the DE4A piloting project (https://www.de4a.eu/about-project). This project is funded by the European Commission. It aims to explore ways to implement and provide once-only e-government services, particularly in the context of the Single Digital Gateway. The objective is to ensure that e-government services work more efficiently, securely and smoothly.

All services and applications in this pilot are offered in a test stage only. While they aim to present a realistic user experience, they are not intended to create binding legal effects for the users or for any third party, nor can they be used to satisfy any legal or procedural requirement at this stage. If you wish to create such legal effects or to complete procedures in a legally compliant manner, please do not rely on the pilot services and applications at this stage.

By using these services and applications, you agree to participate in the DE4A pilot on a voluntary basis. Your data will be handled securely by the participants in this pilot, and will only be used to assess whether it is possible to use the pilot services and applications successfully, including by monitoring use of the services and applications for any errors, and analysing user behaviour.

The pilot projects are principally managed by the organisations identified on the DE4A project page, who will act as data controllers in relation to your data. For any questions in relation to the pilots or to your data, please contact them directly, or alternatively contact the DE4A project via [[1]].

4.2.2 Standardised disclaimer for live piloting

The services and applications provided as a part of this pilot have been set up in the context of the DE4A piloting project (https://www.de4a.eu/about-project). This project is funded by the European Commission. It aims to explore ways to implement and provide once-only e-government services, particularly in the context of the Single Digital Gateway. The objective is to ensure that e-government services work more efficiently, securely and smoothly.

The services and applications are designed to be fully functional and operational, and will produce binding legal effects for you, and for any persons or organisations that that you interact with. Therefore, please use the services and applications only if you indeed aim to complete a legally valid procedure.

The services and applications are created with the highest level of diligence, to ensure that they work in a secure and problem free manner. None the less, since they are operated as a part of a pilot, your use of the services and applications is proactively monitored and analysed in order to detect any problems. We may therefore use any contact information you provide to contact you in case of any problems.

The pilot projects are principally managed by the organisations identified on the DE4A project page, who will act as data controllers in relation to your data. For any questions in relation to the pilots or to your data, please contact them directly, or alternatively contact the DE4A project via [[1]].

4.2.3 Privacy policy

DE4A privacy policy for [name of the pilot service, as used on the microsite]

This privacy policy applies to our use of any and all personal data collected by us or provided by you in relation to this pilot. Your use of any services and applications in this pilot will result in the processing of certain personal data relating to you (as the user of the pilot), or possibly relating to third parties (if the service or application requires personal data from such third parties to be processed). While DE4A is a pilot project, it is set up to comply fully with European data protection law, including specifically *the General Data Protection Regulation (GDPR). Through this privacy policy, we aim to inform you of how your data will be used and protected, as required by law.*

***Please read this privacy policy carefully*.**

Who we are and how to contact us

Each pilot project in DE4A is principally managed by the organisations identified on the specific website of that pilot, in this case [URL to the microsite of the relevant pilot]. The organisations that you are interacting with in the context of your participation in the pilot will act as data controllers in relation to your data. When this privacy policy refers to 'us', 'we', or 'our', it refers to the organisations that you'll interact with during your participation in the pilot.

For any questions in relation to the pilots or to your personal data, please contact them directly using the contact information provided on the piloting website; or alternatively contact the DE4A project and its data protection officer via [[1]], and we will help to identify the relevant parties for you and/or address your questions.

Personal data and our use of it

During the course of piloting, we will explore ways to implement and provide once-only e-government services, particularly in the context of the Single Digital Gateway. The objective is to ensure that e-government services work more efficiently, securely and smoothly.

To do so, we may ask for certain personal data from you, or obtain it from you automatically. Specifically:

- You may choose voluntarily to register to participate in our piloting activities. In doing so, rudimentary contact and identity details relating to you and/or the organisation(s) that you represent may be requested.

- You may choose voluntarily to answer questionnaires relating to our piloting activities, e.g. to provide us with more details on your profile, expectations, needs, and requirements. In doing so, rudimentary contact and identity details relating to you and/or the organisation(s) that you represent may be requested, as well as your personal feedback.

- You may choose voluntarily to use the pilot services and applications in order to simulate a realistic but fictitious use case, or (if available) to actually complete a legally valid procedure. Whether the procedure is simulated or real will be clearly and unequivocally communicated to you in advance. In doing so, all personal data required to complete the procedure will be requested from you, including identity information and any additional information required to demonstrate your eligibility for the procedure, and your adherence to any applicable requirements. Any such required information will be explicitly communicated to you before you share it with us, and you will have the opportunity to review it and (if you desire) to terminate the procedure at any time.

In addition to personal data that you actively provide to us, we will also automatically collect personal data relating to your user experience, including detailed logs on your activities during piloting, data made available by you or by third parties, and metadata such as your IP address, device information, session date and duration, and success or failure logs. This data is collected and proactively analysed by us, since the applications and procedures are in pilot status, and we must ensure that no adverse effects can occur for you or for third parties. This data will therefore not only be used to complete the pilots, but also to evaluate risks and problems, to measure performance and satisfaction, and to improve piloting across iterations.

Please note that ***your participation in the pilots is never obligatory.*** *There are always non-pilot alternatives to completing the relevant legal requirements, and there is never a negative repercussion if you prefer not to participate. Your data will not be used for automated decision-making, including* *profiling, except where a pilot service is used to complete a real life administrative procedure that is fully automated. In the latter case, the protections of European data protection law will be applied fully by the applicable public administration.*

Personal data processed by us during piloting will principally relate to you. Depending on the pilot application however, you may need to provide personal data relating to third parties (such as e.g. your employees or your family members, depending on the pilot). Please ensure that you are legally permitted to engage in the pilot prior to proceeding, in the same way as for any other public service applications.

We will not share your personal data with parties other than those participating in the pilots as identified above and their service providers, nor will any third parties be permitted to use your data for other purposes than those mentioned above.

Our legal basis for processing your personal data in the context of piloting applications and services is your consent (in relation to your own personal data that you choose to provide to us), and the necessity of processing for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (for the performance of public sector services). Insofar as our processing is based on your consent, you may choose to withdraw your consent at any time by sending a notification to the contact details mentioned above.

Your rights and how to exercise them

You have the following rights in relation to your personal data, where applicable:

a. Right to access - the right to request (i) copies of the information we hold about you at any time, or (ii) that we modify, update or delete such information.

b. Right to correct - the right to have your data rectified if it is inaccurate or incomplete.

c. Right to erase - the right to request that we delete or remove your data from our systems.

d. Right to restrict our use of your data - the right to "block" us from using your data or limit the way in which we can use it.

e. Right to data portability - the right to request that we move, copy or transfer your data.

f. Right to object - the right to object to our use of your data including where we use it for our legitimate interests.

Note that we may ask for proof of your identity, and that the applicability or consequences of your exercising of your rights may vary depending on the piloting context. By way of example: if you choose to use a pilot service to complete a real life administrative procedure, you will not be able to undo this procedure by exercising your data subject rights.

To make enquiries, or to exercise any of your rights set out above, please contact us via the contact information provided above.

If you are not satisfied with the way a question in relation to your personal data is handled by us, you may refer your complaint to the relevant personal data protection authority in your own country of residence.

Personal data retention

Unless a longer retention period is required by law, we will only hold your personal data on our systems for the period necessary to fulfil the purposes outlined in this privacy policy. For fictitious piloting, your data will be deleted at the end of the DE4A project at the latest. Note however that, if you choose to use a pilot service to complete a real life administrative procedure, retention of your data outside of the context of piloting will be determined by the laws applying to the relevant administrative authority.

Transfers outside the European Economic Area

Personal data which we collect or obtain from or via you will not be stored, processed in or transferred to countries outside of the European Economic Area (EEA).

4.3 Ethical requirements, data protection, and Data Protection Impact Assessment

4.3.1 Ethical assessment of DE4A

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. This assessment applies a structure of six value domains, each of which warrant specific scrutiny in DE4A:

- **Dignity**, notably individuals’ right to be secure in their physical and mental integrity.
- **Freedoms**, comprising the rights to data protection and privacy, but also intellectual freedoms (education, expression, thought, religion and information) and social freedoms (assembly, marriage, asylum and property);
- **Equality**, including non-discrimination and rights of minorities and of societally more vulnerable parties;
- **Solidarity**, covering workers’ rights and labour rights, social security, collective bargaining, health care and environmental protection;
- **Citizens' rights**, such as the right to vote, to proper administration, access to documents and freedom of movement;
- **Justice**, including access to fair trial and effective remedy, and the right to defence.

These values collectively comprise the normative framework to be applied as a yardstick to DE4A. Based upon the conducted ethical evaluation (which can be found in detail in D10.5), the Ethics Advisor noted that the current actions and plans of the DE4A project are in line with the EU’s ethical requirements, but identified two ethical challenges that should be monitored and evaluated as priorities:

- With respect to **data protection**, the report noted that some DE4A piloting activities would not remain strictly within the confines of the SDGR, referring to the alternative interaction patterns explored in DE4A. To address this point, it strongly recommended that a data protection impact assessment (DPIA) would be conducted to mitigate data protection challenges.
- With respect to **equality and citizen’s rights**, including the right to good administration, the report recommended to implement a mature governance framework to ensure that piloting risks could be appropriately monitored and mitigated. From an operational perspective, this was already done via the governance model within each pilots, requiring pilot specific coordination between pilot participants, and escalation/coordination procedures towards the DE4A Executive Board. From a legal perspective, this recommendation was implemented via the DE4A Memorandum of Understanding (MoU).

For this reason, the DPIA and MoU are pillars of the legal and ethical outputs of DE4A, both of which are integrated and commented below.

4.3.2 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 required by the GDPR, a DPIA must contain:

> (a) a systematic description of the envisaged processing operations and the purposes of the processing
>
> (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes
>
> (c) an assessment of the risks to the rights and freedoms of data subjects
>
> (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR

Each of these topics is systematically addressed and described in the current DPIA. It concluded that DE4A operates within the boundaries of data protection law and European ethical standards. The full text of the DPIA as completed at the time of submission of this deliverable is included in Annex I.

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. The DPIA will be adapted when processing operations and/or the resulting risks evolve.

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

4.4.1 General approach and concept

As noted above, piloting activities in DE4A are partially organised within the context of the SDGR, but they also aim to generally pilot solutions based on innovative technologies that enable new forms of organising once-only transactions in cross border e-government use cases (irrespective of whether they fall witing the scope of the SDGR). This raises certain challenges for some piloting partners in the DE4A project, since the legal rights and obligations of the partners are not comprehensively regulated. The SDGR will not become fully applicable until December 2023, and some piloting activities will not be covered by the SDGR. While the DE4A Grant Agreement and the DE4A Consortium Agreement provides a legally binding statement of the rights and obligations of DE4A partners, these do not address constraints and obligations in relation to piloting to any level of detail.

In the absence of sufficiently comprehensive legislation or contracts, it is not unambiguously clear what the limitations to piloting activities in DE4A might be, nor how piloting partners are expected to be organised. The purpose of the Memorandum of Understanding (MoU) is to fill this gap, by 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.

As was also the case for other Large Scale Pilot projects in the EU, an MoU was thus drafted, circulated and approved by the DE4A partners. A full copy of the MoU can be found in Annex II.

Briefly summarized, the MoU implements a risk-based governance mechanism, requiring pilot participants to evaluate what the risk is in each piloting activity. It recognises three principal risk levels:

- 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.

The risk qualification must be documented and justified for each pilot, and specific legal and ethical safeguards are implemented for each level (covering interaction between the parties, communication with users, monitoring, and DPO involvement, among other points). In this way, a coordinated governance approach is created for all DE4A piloting activities.

4.4.2 Status at the time of submission

The MoU is intended to be signed by all DE4A partners who are involved in piloting, i.e. in any activities that involve the exchange of evidence to satisfy administrative procedures targeted by the DE4A pilots. Any DE4A partner may opt to allow this MoU to also be signed by other parties who are involved in such piloting activities on their behalf (e.g. subcontractors to the piloting partners).

Piloting parties may state their intent to adhere to the terms of the MoU by signing the Statement of endorsement within the MoU. An overview of signatories is kept on the DE4A legal wiki. At the time of signing, 11 DE4A partners have already signed and submitted the MoU, out of 16 expected signed copies. Additional signatures are expected before piloting initiates.

5 Topics for future reflection

5.1 Introduction

The objective of this deliverable is to present the central legal and ethical topics that have been under discussion within the consortium, and captures the main efforts undertaken to adhere to the terms of the SDGR and other legislation at the time of submission, and to satisfy ethical requirements, including but not limited to data protection. The sections above summarised 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.

However, this Chapter of the deliverable aims to also provide a concise prospective discussion of legal and ethical topics for future policy reflection. This is an initial description of areas where new legal or ethical reflection may need to occur in the future, since some of the experiences in DE4A exceed the current legal vision of the SDGR. The future discussion topics do not contain a consensus position from the entire consortium on desired outcomes, but rather aim to signal points where there is legal or ethical margin for evolution in the future. These will be further developed in the next iteration of this deliverable (D7.3, due in M30 of the project), as more knowledge is accrued.

5.2 Key legal and ethical topics for future reflection

5.2.1 Once-only exchanges for public policy benefit

A first legal and ethical topic that warrants future attention is the notion of how the OOP is interpreted, scoped and legislated. As was already described above, the SDGR supports only one specific concept of once-only exchanges: those requested by the user. While there is still some margin of interpretation (would a user be able to request / authorize exchanges over an extended period of time?), the core notion is that the user is in charge. Without a prior request, no evidence can be exchanged. Prima facie this is beneficial, certainly from a data protection perspective, but even from a quality of governance perspective: since the user always intervenes in SDGR evidence exchanges[8], in an online session where they are identified and authenticated, exchanges can only occur with user knowledge, and with their ability to verify, control and block data exchanges. This makes it significantly less likely that errors will occur.

None the less, there is an ethical trade-off. This approach implies that once-only exchanges cannot be done proactively without user involvement, even if this would be beneficial from a public policy perspective. The examples given above can be repeated: because of this approach, evidences could not be exchanged that would e.g. allow a citizen to automatically get access to specific benefits such as subsidies. In other words, users can become victims of suboptimal once-only information exchanges, merely because they are unaware that they could and should apply for a benefit. This is all the more ethically fraught, because this negative impact is stronger for persons with lower familiarity with administrative procedures and digital transactions. In other words, it will be particularly negative for persons who are most at risk. This issue warrants further reflection.

The second example given above is perhaps more intuitive: users could choose to authorize exchanges of evidence at a time that is beneficial to them (e.g. at a time when they qualify for a specific benefit), even though they know that they will become ineligible for that benefit soon thereafter. Since the SDGR does not allow updates to be sent without a user request (e.g. to communicate that a user should no longer receive a contract or be permitted to perform a specific job), the once-only exchanges are not ideal for detecting errors, oversights or fraud attempts. Arguably this is by design and the privacy

[8] Thus excluding lookup and subscription/notification patterns, which are both exempt from the request obligation (in the lookup case because it relates to publicly available data; and in the subscription/notification case because no evidence is exchanged).

benefit outweighs the negative externality; but none the less it is a choice that has negative implications, the costs of which are borne by society as a whole.

These considerations do not imply that the scoping of the SDGR is faulty; but rather that potential benefits are lost with the current constellation. This merits follow-up debate.

5.2.2 Data sovereignty of the user

A second issue is the role of the user. The SDGR grants the user a central role, as the gatekeeper of their data. Via the request and preview mechanism, they trigger or block evidence exchanges between competent authorities (assuming that there is no other legal basis, since both the request and preview are subject to exceptions, as is extensively commented in D7.1).

However, the once-only exchanges envisaged by the SDGR are fairly traditional, in the sense that the SDGR requires evidence to be exchanged between competent authorities. In a very fundamental way, the evidence remains under the control of competent authorities: they hold the original data, and provide it to other authorities upon request of the user. They do not provide it to the user as such. The user is a gatekeeper, not a sovereign.

This is a defensible policy choice, and in line with the main thinking behind once-only exchanges in the public sector. If the intention is to unburden the citizen, the objective should not be to merely hand data to them, and simply require them to handle the next steps themselves – that could increase complexity for the user and introduces new legal and ethical challenges. If a user would indeed be able to request and hold their own data, e.g. in a secured locker or on their smartphone, the risk is that the SDGR would not be used to orchestrate the procedures that fall within its scope, but rather that it becomes a generic tool for transparency, for freedom of information requests, or even for personal data access rights as enshrined in the GDPR. In other words, emphasising personal data sovereignty in such a way – by allowing users to hold their own data – could create new problems that exceed the potential benefit.

None the less, this is an issue that will require further policy attention in the future as well, not only because DE4A aims to pilot verifiable credential patterns (which lend themselves extremely well to data sovereignty models), but also because the contemplated amendment of the eIDAS Regulation aims to introduce a legal framework for European Digital Identity Wallets, that could be used for (among other functions) storing electronic attribute attestations – in other words, verifiable credentials. Given that the SDGR builds on the eIDAS framework, this potential "value clash" between personal data sovereignty and once-only based governance merits further discussion.

5.2.3 Identification and integrity/authenticity approaches

One of the challenges in implementing once-only exchanges at the cross-border level is ensuring the identification of the users, and ensuring the integrity and authenticity of exchanged information. The eIDAS Regulation is the principal legal building block on this topic in the European Union.

However, the eIDAS Regulation is not perfectly capable of addressing all relevant challenges. To enumerate only a few examples:

- The eIDAS Regulation does not ensure that each citizen has only one notified electronic identity across the EU, nor that the multitude of electronic identities that they may have can be mapped cleanly. I.e. a citizen who has multiple electronic identities in accordance with the eIDAS Regulation (e.g. a Spanish ID card because they were born there, a Belgian one because they are domiciled there, and an Austrian one because they have a residence there) can use all of these identities in parallel. Public administrations have no conclusive means of mapping the identities against each other. This is complex for the user, and creates risks for mistakes and fraud.
- The eIDAS Regulation does not offer a sufficiently comprehensive framework for the representation of legal entities. Partially this is due to the simple problem that types of legal entities and types of representatives and their legal competences are currently defined at the Member State level.

Company types are thus different from Member State to Member State, as are the types of persons who can represent them. In this constellation, the maximum achievable outcome is the validation that a specific natural person has a specific legally defined title in a legal entity – without however being able to substantively assess what that title entails, or which competences are included under that title.

- Comparably, the representation of natural persons (e.g. a parent towards their children, or a guardian towards persons with mental impairments) has no clear legal framework at this stage. While this may appear a minor problem, it also implies that common cases (a parent enrolling their minor child at a school, or a guardian changing the residence of their ward) cannot be implemented, especially at a cross border level as envisaged by the SDGR.

No easy and comprehensive solutions are available to these problems. Of course, DE4A maximally aligns with best practices and prior developments. Specifically, DE4A integrates the SEMPER extensions to eIDAS, that were developed and tested in earlier projects. The SEMPER extensions facilitate the determination whether an identified natural person has a defined legal role in a given legal entity. The approach is functional and reliable in practice, although it has no specific legal authority, and cannot resolve the aforementioned problem (assessing exactly what a role entails of what competences are included). Thus, while DE4A optimally reduces risks by building on earlier initiatives, it should be recognised that the lack of a clear answer on these topics creates potential discriminations between persons that should have identical rights, which is both legally and ethically challenging.

5.2.4 Semantics, translation and legal validity

Next, a potential challenge for once-only exchanges is the interpretation of exchanged evidences. The objective of the SDGR (and of the OOP in general) is to ensure that evidences can be exchanged and further processed easily in cross border scenarios. That can only be done if the contents of evidences can be easily interpreted. Beyond the issue of evidences requiring a certain logical structure to achieve this goal (as discussed in section 3.4 of this deliverable), the structured information must also be understandable for the recipient. This is an issue of semantics.

This issue can be partially resolved through appropriate semantic mapping and through machine translation, and this is indeed the approach that will be applied by DE4A as well. However, it should also be recognized that this creates a new legal and ethical risk. The authentic evidence is the original evidence issued by a competent authority. If technical services convert this evidence into a different format – through translation and/or semantic mapping to presumably comparable concepts – then this converted evidence is no longer authentic. In a paper environment, this issue was addressed through the slow and costly processes of sworn translation and notarization (among other approaches). If the objective is to replace these procedures by quick and easy automated processes, then this needs to be appropriately regulated as well, to protect receiving administrations against inappropriately or incorrectly transmuted evidence.

This issue presently has no clear resolution. This is all the more legally and ethically challenging if the evidence will be functionally presented to the requesting authority in a structured and semantically converted manner, that will be significantly easier to use than the original authentic evidence. If that approach is followed, a moral hazard is created, where a requesting authority knows (or should know) that only the original evidence is legally valid, but is induced and encouraged to instead rely on the transmuted form.

6 Conclusions

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 Memorandum of Understanding and DPIA).

It is also clear that significant work still lies ahead. Part of the challenge is the fact that the SGDR's Implementing Act has not yet been finalised so that legal requirements may still evolve, and that the legal framework of the eIDAS Regulation is similarly undergoing amendment to support (among other topics) mobile identification, attribute certification / verifiable credentials, and digital ledgers, all of which may play a role in DE4A and in future OOP work.

Moreover, as the previous chapter has shown, there are open prospective issues for which no conclusive answer or consensus position is available yet.

Finally, piloting work is still to initiate in DE4A, and it is clear that new experiences will require modification as new insights emerge. For that reason, much of the work in this deliverable is still subject to evolution. This is not unexpected, and the Grant Agreement foresees that this D7.2 must be maintained and updated into a final and conclusive D7.3, due in the last months of the project. It is therefore intended that the findings of this report and its outputs will be further refined and adjusted, based on future discussions and working experiences in DE4A.

7 Annex I – DE4A DPIA

7.1 Introduction and scope

7.1.1 Impact assessments under the GDPR

This DPIA has been drafted to assess data protection risks within the DE4A project, with the objective of mitigating them as far as possible, in accordance with the requirements of the General Data Protection Regulation.

The methodology has been designed in accordance with the requirements of the Article 29 Working Party's Guidelines on Data Protection Impact Assessments [9]. As these Guidelines indicate, a DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them.

DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation. In other words, a DPIA is a process for building and demonstrating compliance.

Methodologically, DPIAs should at a minimum contain:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

While some of these topics are partially common to all DE4A pilots since they are addressed via the general DE4A architecture, the context of individual pilot areas is a relevant factor in determining risks and impacts on data subjects. For this reason, the DPIA is conducted at the level of pilots, not on the project as a whole.

The DPIAs will be maintained and further developed iteratively in the course of the project, to ensure that they remain fully aligned with the realities of the project.

7.1.2 Prior inputs – Commission DPIA for the SDGR

The DE4A project takes place against the backdrop of the Single Digital Gateway Regulation (SDGR) [6]. 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 the 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, among other avenues to piloting the once-only principle.

Globally, the SDGR reflects a specific perspective on the OOP, where exchanges are driven by user requests, under specific safeguards defined in the SDGR. These safeguards are to be further elaborated via an Implementing Regulation, for which the European Commission has been working on a proposal. This proposal was accompanied by a separate DPIA [5], conducted by the Commission staff, that examined the following topics of the SDGR and the Implementing Regulation in particular:

- Legal basis
- Explicit request
- Preview requirement
- Authentication of the user and mapping a user to evidence
- Security and confidentiality during the transmission of data
- Principles of purpose limitation and data minimisation
- Storage limitation
- Security by design
- The role of the Member States and the Commission

Based on an assessment of these topics, as addressed by the SDGR and the proposed draft Implementing Regulation, the DPIA concluded that "*The OOTS as designed in the draft Implementing Regulation complies with the relevant provisions of the SDGR and the data protection requirements, while ensuring the user friendliness of the system which is essential to guarantee the use of the system*".

The current DE4A DPIA builds upon this Commission DPIA, adding considerations specific to the DE4A architectural choices and to the selected piloting activities. Moreover, the present document aims to assess risks related to data processing activities in a more structured and systematic manner. All safeguards identified in the Commission DPIA (which are not repeated in the present document) remain applicable and will be complied with by DE4A as well.

7.1.3 The once-only principle, DE4A and e-government beyond the SDGR

One of the key objectives of DE4A is to establish piloting solutions for the technical system as envisaged by the SDGR. For that reason, the requirements established by Article 14 of the SDGR are crucial inputs to determine the legal constraints for the DE4A project. However, 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 requirements. These will be described and evaluated in this DPIA as well.

7.2 Scoping – description of the processing operations being assessed

7.2.1 General note on the scoping of this DPIA

The DE4A project's ethics requirements are managed in detail within Work package 10 - Ethics Requirements. Further information can be found in the relevant deliverables, notably:

- D10.1 Requirement n°1 – Identification and recruitment of participants
- D10.2 Requirement n°2 – Data Protection Officer
- D10.3 POPD Requirement n°3 – Further processing

For the scoping of this DPIA, a key consideration is that the DE4A project builds on the policy background of the adopted SDGR, and of the 2017 Tallinn e-government declaration, which emphatically supported user driven once-only exchanges as a pillar of future e-government policy. As such, DE4A is a digital government project which aims to facilitate the electronic exchange of information in administrative proceedings where this information thus far is usually done on paper.

Therefore, DE4A does not aim to create new data flows (exchanging information where no information was exchanged before), but rather to create a new way to organise existing data flows, in the context of existing and regulated procedures, conducted by existing regulated public authorities. Similarly, the once-only principle is not a DE4A choice or initiative, and to a significant extent the execution of DE4A is scoped and limited by pre-existing work.

This also limits the scoping of the DPIA within the project, since DE4A's remit is not to assess the data protection compliance behind the choices made in the SDGR, or in the Tallinn Declaration, nor the administrative procedures organised by Member States. The DPIA focuses on DE4A's data processing choices only. In other words, DE4A must reasonably assume that the SDGR, the existing administrative procedures, and any existing EU level building blocks are compliant with data protection law already, and limit itself to the implementation choices that the project itself makes.

For this reason, the DPIA does not assess the once-only principle as described in the SDGR, nor the adequacy of safeguards foreseen in the SDGR and the Implementing Regulation – on those topics, we refer to the Commission's DPIA. Similarly, the DPIA does not assess national systems or procedures that exist already prior to the DE4A project, nor the CEF Building Blocks that are integrated into the DE4A architecture and pilots.

7.2.2 DE4A general data flow description

A data flow assessment is a preliminary step to the preparation of a DPIA. The assessment should allow the identification of the main elements of a planned or tentative processing activity. One of the objectives of DE4A is to design a solution for the technical system of Article 14 of the SDGR, and thus a solution to implement the SDGR's perspective on the OOP. Deliverable 2.1 Architecture framework [13] and D2.4 Project Start Architecture (PSA) – First iteration [14] discuss several possible patterns to implement the OOP, most of which will be piloted to some extent.

In terms of data protection:

- The data exchange covers several categories of personal data, depending on the administrative process undertaken.
- The purpose of the processing is the transfer of administrative evidence necessary to the accomplishment of specific administrative procedure, as defined in national or European legislations.
- The typical legal basis is the necessity of processing for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller' (article 6.1 (e) GDPR). Complementary legal bases might be found in the consent of the users, but an appeal to consent is neither strictly necessary nor universally beneficial.
- The processing supposes several transfers:
  - In the request for evidence: the data consumer must send the information necessary for the data provider to identify the evidence to be sent.
  - In the response: the data providers transfer the evidence, and therefore the personal data it contains
  - The preview mechanism: the data is transferred, or made available to the data subject for validation

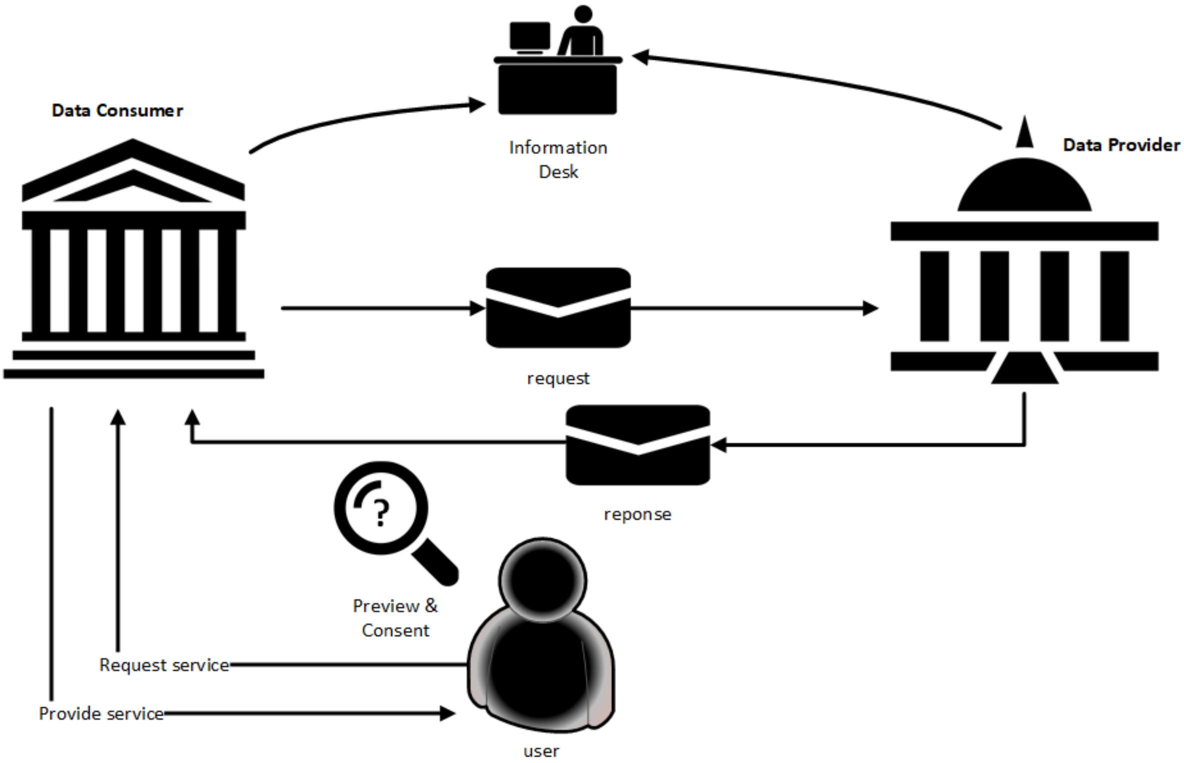

Figure 1: Primary intermediation pattern, see D2.1[13]

The primary intermediation pattern is the basis of the implementation of the OOP through the technical system of the SDGR. However, this is not the only available option; other and arguably more user centric designs are also possible and are being investigated in DE4A. These are described in detail in D2.4 Project Start Architecture (PSA) – First iteration [14]; and include notably:

- Intermediation Pattern, in which the data consumer orchestrates all interactions with the user;
- User-supported Intermediation Pattern, in which the user also interacts directly with the data provider in order to obtain the relevant evidences;
- Verifiable Credentials Pattern, in which evidences are made available in the form of Verifiable Credentials (VC), i.e. digital data representations about the user in the form of a set of claims. Verifiable Credentials can be cryptographically verified by any third party, including the data consumer in the context of a DE4A pilot.

As will be shown below, the User-supported Intermediation Pattern is currently by far the most common pattern in DE4A, being applied in all but two use cases. The considerations behind this choice will be explored below.

Two additional Reference Interaction Patterns are considered in later iterations, notably:

- Subscription and Notification Pattern
- Lookup Pattern

These are not yet integrated in the present DPIA, since these have not yet been fully elaborated.

7.2.3 Pilot specific elements

Three piloting streams are examined in DE4A, covering several use cases: Studying Abroad Pilot (SA), Doing Business Abroad Pilot (DB), and Moving Abroad (MA) Pilot. Without going into detail at the present stage, this section provides an overview of piloting plans. For more detail, we refer to the Pilot Plans (D4.2 Studying abroad Pilot planning; D4.6 Doing Business Abroad pilot planning, and D4.10 Moving abroad pilot planning, respectively) [15][16][17].

7.2.3.1 Studying abroad

This stream contains a combination of three use cases (Application to public higher education, Applying for study grant, and Diploma recognition)

Categories of data subject include: students, prospective students, and former students.

Table 1 : Categories of personal data used in the Studying abroad pilot

SDGR Procedure	DE4A Studying Abroad pilot use case & Exchange pattern	Categories of data used
Submitting an initial application for admission to public tertiary education institution	Use case 1: Application to public higher education User-supported Intermediation Pattern	Personal identification data, Government issued identification data Information concerning higher education
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 User-supported Intermediation Pattern	Personal identification data, Government issued identification data Information concerning higher education Information concerning family members Financial identification data Financial resources Financial assistance
Requesting academic recognition of diplomas, certificates or other proof of studies or courses	Use case 3: Diploma / Certs / Studies / Professional Recognition Verifiable Credentials Pattern	Personal identification data, Government issued identification data Information concerning higher education

The use cases can rely to a significant extent on interaction with the user for data protection safeguards, since all personal data involved relates exclusively to the user. Most of the personal data is not highly sensitive, with the exception of any required information on financial background that may be asked to determine eligibility for grants.

Use case 3 (Diploma / Certs / Studies / Professional Recognition) is the only use case currently planned to apply the Verifiable Credentials Pattern. This is a logical choice, since in a paper environment, diplomas (or other documents showing professional qualification) are normally also held by the user itself. Moreover, they are relatively static documents since diplomas generally do not become invalid over time, are not significantly sensitive, and are commonly shown to third parties (e.g. in the context of job applications or other HR procedures). This makes the use case highly suitable for the VC pattern.

7.2.3.2 Doing Business Abroad

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), but personal data is inevitably involved, relating to representatives of legal entities and their personnel. More specifically, the data concerns the natural person (representative), the company (represented) and the relationship between both (the powers).

In exceptional cases, it is conceivable that the exchanged evidence does not contain any personal data at all – e.g. in case of large companies who exchange only company data, and even contact information is provided at the functional and non-personally identifiable level. None the less, GDPR compliance also must be taken into consideration for the Doing Business Abroad pilots.

The DBA pilot uses the basic Intermediation Pattern only.

For reasons of risk management and complexity management, the use case is not expected to pilot situations where the representative's nationality does not match the country of establishment of the legal entity (i.e. a Dutch national will be able to represent the Dutch companies for which (s)he is a designated representative, but not any companies established in other Member States).

To handle representation competences in relation to a legal entity (i.e. the question of determining for which purposes a natural person with a predefined mandate can legally engage the entity), the use case relies on the SEMPER initiative and its outcomes. Since no structural ontology of competences and mandates exists, the piloting activities will rely on general rights of representation, i.e. the presumption that an identifiable legal mandate will be valid without constraints for the purposes of piloting.

7.2.3.3 Moving Abroad

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

Table 2: Categories of personal data processed in the Moving Abroad pilot

SDGR Procedure	DE4A Moving Abroad pilot use case & exchange pattern	Categories of data used
Registering change of domicile address	Requesting a change of address User-supported Intermediation Pattern	Personal identification data
Citizens' and family rights	Request an Extract or Copy of a Civil State Certificate User-supported Intermediation Pattern	Personal identification data Information on civil status
Requesting information on the data related to pension from compulsory schemes	Request Pension Information - Claim Pension User-supported Intermediation Pattern	Personal identification data Personal particularities Particularities regarding pension Professional employment *Note: 2nd iteration may include information regarding health (e.g. disability information). This is not yet considered in this iteration of the DPIA*

The principal challenge, beyond the inherent sensitivity of some of the data, is the potential effect on third parties: a person aiming to change their domicile address may e.g. require or expect to also be able to change the address of a spouse and/or child. For reasons of risk management and complexity management, the use case is not expected to pilot representation of spouses – all legal adults will be required to represent themselves individually – nor situations with complex family links – an adult may represent their children, but there is no guarantee or objective of ensuring that the system will also work in cases of e.g. legal guardianship, or in relation to adults for whom parents still exercise parental authority (e.g. due to mental impairments), or in situations where a child is not known or registered in the country of residence of the parent (e.g. because the child was born abroad, and never moved countries along with their parent).

7.3 Assessment of the necessity and proportionality of the processing operations in relation to the purposes

A DPIA must consider the necessity and proportionality of all processing operations in relation to the purposes of data processing. If the purposes can be achieved through means that require no processing of personal data, or that would require less (or less sensitive) processing of data, then the alternatives should be implemented.

In the case of DE4A, the purposes of processing are determined entirely by the piloting objectives as described in the use case descriptions above. For comprehensiveness, it should be stressed that this necessity relates to the data controllers, i.e. the legal entities participating in the DE4A project as piloting partners, who are legally committed to organising piloting activities under the DE4A Grant Agreement. The processing activities are kept as minimal as possible (both in terms of the scoping of personal data processing, and in terms of exposure of the data to participants in the pilots) to ensure that the piloting can take place in a useful setting. The piloting activities also serve a public interest objective, given that they are necessary to ensure that the SDGR can be implemented in a timely fashion, as required by the European legislator. Thus, the processing operations are necessary and proportionate.

For the avoidance of doubt, the processing operations (i.e. the piloting activities in DE4A) are not necessary from the perspective of the users themselves, whose personal data will be processed. However, in accordance with the principles of the SDGR, no individual will be required to participate in piloting activities. As has been explained in the scoping section, DE4A does not create new administrative procedures, but only a new (and hopefully superior) way of satisfying existing procedures. A citizen who does not wish to engage in piloting activities will always have the option of following traditional procedures, separate from the DE4A project.

Based on this assessment, the processing operations in the piloting activities are necessary and proportionate.

7.4 Assessment of the risks to the rights and freedoms of data subjects

7.4.1 General introduction on risks to the rights and freedoms of data subjects

The objective of a DPIA is to identify and mitigate risks that exist in relation to the targeted data processing activities. As described by European data protection authorities in their official guidance [9], a "risk" is a scenario describing an event and its consequences, estimated in terms of severity and likelihood. Consequently, this DPIA should identify such events and consequences, along with an estimation of the severity and likelihood.

In order to do so, it should be emphasised that a DPIA examines risks "to the rights and freedoms of individuals" – not to organisations, technical systems, processes or procedures. Examples of risks with an impact on rights and freedoms of individuals include:

- illegitimate access to data (loss of confidentiality);
- unwanted change (loss of integrity);
- disappearance (loss or corruption) of data (loss of availability);
- disproportionate collection of data;

- unlawful monitoring or crosslinking of data
- inadequate transparency on data collection, use or access
- disregard of data subject rights (loss of access or deletion rights)
- unlawful data sharing or re-use
- disproportionate retention

Risks for organisations, technical systems, processes or procedures can be included only if they are presented from the perspective of the data subject.

In the table below, we summarise the main risks identified by the DE4A consortium in relation to the planned DE4A piloting activities. As noted above, the assessment does *not* focus on risks inherent to the SDGR, or risks related to existing building blocks for e-government, or risks related to purely national data processing practices. When describing risks, the fact that other Member States lawfully use data differently than in the citizen's home country is therefore not considered a risk in this DPIA.

The table also provides an assessment of the severity and likelihood of risks, based on the opinions of DE4A participants, and identifies at a high level whether and how any risks have been mitigated.

7.4.2 Overview table of identified piloting risks and mitigation measures

7.4.2.1 Identified and mitigated risks

Table 3: Overview table of identified piloting risks and mitigation measures

Description of the data protection risk	Likelihood (low, medium, high)	Severity (low, medium, high)	Applicable to all pilot areas, or pilot specific?	Have the risks been mitigated? Are any risks remaining?
Identity mapping of the user between public administrations relies on an imperfect model. There is no unique mappable identifier, and thus no perfect guarantee that the evidence relates to the exact user.	Low	High	All pilots	Some mitigation is implemented and piloted through best practices for identity mapping, building on fuzzy logic; but risks remain. The Commission DPIA recognises this risk, but provides no clear solution other than delegating the definition of an approach to the Member States. The User-Supported Intermediation and Verifiable Credential patterns mitigate this too, since they require (respectively) re-identification towards data providers and autonomous use of VCs that are bound to an authenticated user.
Powers of representation/mandates has no mature system under EU law, both for company mandates (who can legally represent a company?) and for mandates between persons (e.g. parent-child representation rights).	High	Medium	Pilot specific - DBA (representation of companies), and MA (representation of families	Some mitigation exists due to the reliance on national infrastructure (national eID linked to national company registers and national mandate systems); but this becomes difficult cross border. For that reason, DBA does not pilot scenarios involving 3 or more Member States, so within DE4A that risk has been eliminated. Comparably, the MA aims to pilot representation of a child by a parent at the national level (where

Description of the data protection risk	Likelihood (low, medium, high)	Severity (low, medium, high)	Applicable to all pilot areas, or pilot specific?	Have the risks been mitigated? Are any risks remaining?
				relevant data and infrastructure should be available, and there is no issue of cross border diverging laws), but no more complex family representation scenarios. Moreover, DE4A will rely on outputs from the SEMPER project that extend the core eIDAS model, so that it can build optimally on the most state of the art approach in the EU today. Finally, mandates are initially only piloted in a simplified form, relying on general powers of representation in companies, without considering potential nuances or limitations in representation rights; this is simplified as an approach, thus creating uncertainty on legal validity in complex cases; but also eliminating semantic discussions. Piloting (both DBA and MA) can become more complex in future iterations, assuming success in initial iterations.
The SDGR's Implementing Regulation foresees a preview with the data consumer, rather than per data provider. This requires all data providers to maintain perfect compliance with technical requirements, since they all need to be able to communicate with the technical system (they cannot organise previews locally).	High	Low	Only relevant for the basic intermediation pattern (so in DE4A, only for DBA, since the others use USI or VC patterns)	Mitigated through the alternative patterns that eliminate this challenge (but which are not in line with the draft Implementing Regulation on this point). In the DBA pilot, the problem shouldn't present itself, given the controlled environment.

Description of the data protection risk	Likelihood (low, medium, high)	Severity (low, medium, high)	Applicable to all pilot areas, or pilot specific?	Have the risks been mitigated? Are any risks remaining?
SSO requirements towards evidence providers - no reidentification is allowed, reliance on eIDAS identification	High	Low	Only relevant for the basic intermediation pattern (so in DE4A, only for DBA, since the others use USI or VC patterns)	Mitigated through the alternative patterns that eliminate this challenge (but which are not in line with the draft Implementing Regulation on this point). In the DBA pilot, the problem shouldn't present itself, given the national verification of representation rights only.
DE4A can provide both structured and unstructured evidences. For unstructured evidences, both original and canonical evidence are provided, which creates the risk of a mismatch between the two, if the original is incorrectly transformed into canonical evidence (e.g. relevant data is omitted).	Medium	Medium	All pilots except DBA (which only exchanges canonical evidences).	DE4A supports exchange of both types of evidence, which mitigates the problem. This imposes a duty of diligence on the data requester, but this is the same duty that would apply in paper based transfers of evidences, so it is not a new DE4A risk.
Identity fraud could occur by using outdated evidence – in this case, evidence is exchanged successfully, but becomes invalid afterwards; the receiving administration is not notified.	High	Low	All pilots (although relevance and impact are very pilot dependent)	Can be mitigated through the subscription and lookup patterns; but this is not explicitly supported under the SDGR. However, DE4A applies constraints to ensure that evidence is not exchanged without a prior request. For the subscription and notification pattern, DE4A only exchanges information that indicates whether evidence has changed – no evidence as such is exchanged without a prior request. The problem is not too realistic for DE4A, while pilots mainly require instantaneous validation of evidence and instantaneous follow-up. The fact that evidence becomes invalid later is not a significant

Description of the data protection risk	Likelihood (low, medium, high)	Severity (low, medium, high)	Applicable to all pilot areas, or pilot specific?	Have the risks been mitigated? Are any risks remaining?
				risk for DE4A pilots – or at least it is not more significant than for traditional paper based exchanges.
Provided evidence is outdated or inaccurate	Medium	High	Only relevant for the VC pattern, for the purposes of this DPIA	This risk should not be considered for basic intermediation or USI patterns, since the evidence is immediately provided to the data consumer communicated as received. If the evidence from the data provider was already outdated or inaccurate, this is not a DE4A issue. The risk is moreover generally mitigated by the preview requirement, but this is controlled by users only, who may not stop outdated or inaccurate evidence exchanges if the exchange favours them. The issue is mainly relevant for the VC pattern, which inherently creates the risk of users retaining VCs with evidence that has become outdated or inaccurate *after* its issuance. Here too however, the situation is not worse than for traditional paper based exchanges; and the VC pattern can incorporate the ability to verify the accuracy and 'freshness' of the information in the VC.
Where the data provider and data consumer apply separate authentication processes (i.e. in USI pattern), a second person could do the second authentication, thus enabling identity fraud	Medium	High	Only relevant for USI pilots	The risk is more for the data consumer, rather than for the data subject, since in principle the attack requires collusion between two data subjects. While this leads to less reliable data processing, it is not a risk for the data subjects created by DE4A - it

Description of the data protection risk	Likelihood (low, medium, high)	Severity (low, medium, high)	Applicable to all pilot areas, or pilot specific?	Have the risks been mitigated? Are any risks remaining?
				is a risk created by their unlawful behaviour (which may however impact third parties that can also be data subjects). The problem is also mitigated in DE4A through the fact that the USI pattern still requires eIDAS data to be provided, which can be matched in order to detect fraudulent cases. In this pattern, the risk is arguably lower than in traditional paper based exchanges.

7.4.2.2 Rejected risks – i.e. risks that were identified, but which are not retained since they are not specific to DE4A

Table 4: Risk not retained (not DE4A- specific)

Description of the data protection risk	Likelihood (low, medium, high)	Severity (low, medium, high)	Applicable to all pilot areas, or pilot specific?	Have the risks been mitigated? Are any risks remaining?
Data control is removed from the user after the exchange - receiving administrations can use evidence as required by their own laws.	N.A. – rejected risk	N.A. – rejected risk	N.A. – rejected risk	Not a valid risk for the purposes of this DPIA. The risk is inherent to cross border transactions, and not linked to DE4A.
Data minimisation cannot be perfectly implemented - standardised evidences are exchanged, rather than tailored data that comprises *only* the evidence elements that are strictly needed	N.A. – rejected risk	N.A. – rejected risk	N.A. – rejected risk	Not a valid risk for the purposes of this DPIA. Even in a worst case scenario (no filtering of data at all), the problem is not worse than for traditional paper based exchanges. Moreover, DE4A does allow the identification of optional attributes.
Evidence duplication – there can be multiple sources of evidences (e.g. a university or a government database can be sources of data), which could contain conflicting data, leading to “evidence shopping” where a citizen finds the source with the most favourable evidence	N.A. – rejected risk	N.A. – rejected risk	N.A. – rejected risk	Not a valid risk for the purposes of this DPIA. Even if multiple sources would exist (and no such case is known yet in DE4A), the problem would not be worse than for traditional paper based exchanges.

7.5 Summary of measures envisaged to address the risks

Globally, three levels of measures are envisaged to address data processing risks for individuals.

Firstly, there are the measures which are integrated into the legal framework. Article 14 of the SDGR stipulates that the envisaged technical system must contain certain features:

- The user must be able to explicitly request transfer of evidence, thus incorporating requests and request management as a privacy enhancing technology;
- The system must allow the transmission of evidence between competent authorities of different Member States;
- The system 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 transfer to the competent authority, and the user must be able to prevent the transfer if necessary;
- The system must be interoperable with other relevant systems;
- The transfer of evidence must be secure;
- The processing must be limited to what is technically necessary to ensure the transfer of evidence and the evidence must not be stored or processed if it is not necessary for the transfer.

All of these features are integrated into DE4A.

Secondly, there are the measures that are integrated into the DE4A architecture (including the various interaction patterns and pilot specific measures), as described in the table above. It can be noted in particular that some of the interaction patterns are selected and will be piloted specifically because they are expected to be effective in mitigating data protection risks, even if the patterns and measures are not endorsed specifically by the SDGR.

And thirdly, there are the measures that are integrated into DE4A risk management measures. This includes the standardised Memorandum of Understanding (MoU) that all piloting partners are required to sign prior to initiating the pilots. The MoU includes a risk identification approach, that requires risk assessment according to multiple risk levels, and the implementation of corresponding risk mitigation measures, depending e.g. on whether real persons and evidence are involved, or whether piloting occurs on production systems or on pre-production environments. Moreover, DE4A has provided standardised transparency notices and other legal texts to clarify the position of users.

Collectively, these provide a baseline of risk mitigation measures that should be appropriate for DE4A, at a minimum for the first iteration of piloting.

7.6 Conclusions

Based on the currently known and identified risks, and the corresponding risk mitigation measures as described above, the DPIA shows that residual risks to data subjects (i.e. their risks after the implementation of the measures described in this DPIA) are limited, and at any rate **acceptable** for the first iteration of piloting.

As with any DPIA, this report should be updated as piloting evolves, notably when piloting activities result in new or changed risks, and/or when risk mitigation measures are revised. At a minimum the DPIA should be formally revised prior to initiating the second iteration of piloting.

8 Annex II – DE4A MoU

8.1 Introduction

8.1.1 Purpose of this MoU

Within the DE4A project, certain pilots will be organised. During these pilots, evidentiary documents are expected to be exchanged between public administrations and other entities, who are located in different countries. These piloting activities are partially organised within the context of the Single Digital Gateway Regulation (SDGR), but also aim to generally pilot solutions based on innovative technologies that enable new forms of organising once-only transactions in cross border e-government use cases (irrespective of whether they fall witing the scope of the SDGR).

This raises certain challenges for some piloting partners in the DE4A project, since the legal rights and obligations of the partners are not comprehensively regulated. The SDGR will not become fully applicable until December 2023, and some piloting activities will not be covered by the SDGR. While the DE4A Grant Agreement and the DE4A Consortium Agreement provides a legally binding statement of the rights and obligations of DE4A partners, these do not address constraints and obligations in relation to piloting to any level of detail.

In the absence of sufficiently comprehensive legislation or contracts, it is not unambiguously clear what the limitations to piloting activities in DE4A might be, nor how piloting partners are expected to be organised. The purpose of this MoU is to fill this gap, by providing a joint statement of mutual understanding between piloting partners in relation to the requirements, assurances and limitations in relation to piloting.

8.1.2 Legal nature and goals

This document is a Memorandum of Understanding (MoU), not a legally binding contract. It is a non-binding, good faith, statement of shared understanding between the signatories.

Given its legal nature, the Memorandum does not supersede any legislation (whether at the EU, national or other level), nor does it supersede any contractual obligation (including but not limited to the DE4A Grant Agreement and the DE4A Consortium Agreement).

By signing this MoU, the signatories declare their intention to observe the agreements included herein in good faith, and affirm their good faith conviction that, to the best of their knowledge, the terms of this MoU do not contradict any legal requirements that apply to them. If a signatory becomes aware of any reason why he cannot respect the terms of this MoU during the DE4A project, he will endeavour to inform other signatories that may be affected by this inability.

Since the MoU is not a binding and enforceable contract, it contains no terms relating to liability, applicable law, or dispute resolution.

The signatories affirm that the DE4A Grant Agreement and the DE4A Consortium Agreement shall continue to apply to them, and that the terms of the DE4A Grant Agreement and the DE4A Consortium Agreement shall take precedence over any terms of the MoU that could cause a potential conflict.

8.1.3 Scoping and intended applicability of this MoU

The sole objective of this MoU is to support the piloting activities between partners and/or their direct and indirect agents, as described in the Description of the Action (DoA) [18] referenced by the DE4A Grant Agreement and the DE4A Consortium Agreement, and as these may evolve in the course of the DE4A project.

Based on this scoping:

- This MoU does not affect non-piloting activities[9] within the DE4A project
- This MoU does not affect non-piloting partners within the DE4A project
- This MoU does not affect piloting within the DE4A project that's conducted purely internally by only one partner (internal piloting)
- This MoU does not affect any activities (including any piloting) organised outside the scope of the DE4A project
- This MoU terminates automatically after the termination of the DE4A project

The intended applicability implies that this MoU is intended to be signed by all DE4A partners who are involved in piloting, i.e. in any activities that involve the exchange of evidence to satisfy administrative procedures targeted by the DE4A pilots. Any DE4A partner may opt to allow this MoU to also be signed by other parties who are involved in such piloting activities on their behalf (e.g. subcontractors to the piloting partners).

Piloting parties may state their intent to adhere to the terms of the MoU by signing the Statement of endorsement in 8.4, and sending it to the DE4A Executive Board.

[9] To be understood in the broad sense as any activities that don't include any testing of developed components in a way that involves real or fictitious persons or procedures. Non-piloting activities therefor include software development, compilation and black box testing; focus group testing or stakeholder consultation, marketing, feedback collection, surveying and assessing infrastructure prior to piloting, or integration with non-DE4A infrastructure.

8.2 Principles of this MoU

8.2.1 In relation to legal compliance

Given its legal nature as set out in 8.1.2, this MoU does not affect the legal rights and obligations of the signatories. It is not intended to implement, complement or replace any part of the SDGR and/or its implementing act(s). It is also not intended as a precursor to any discussions or negotiations taking place between any signatories of the MoU in the context of the SDGR or in other related policy initiatives. All signatories remain free to take other or contrary positions in such discussions that those which may be included in this MoU.

More specifically and purely by way of example, this MoU does not affect the rights and obligations of the signatories in connection with the SDGR, the GDPR, or adherence to the DE4A Grant Agreement and the DE4A Consortium Agreement. It is not a data processing agreement, partner agreement, networking agreement, or shared policy.

8.2.2 In relation to DE4A outputs

The signatories to this MoU declare their good faith intent to respect any agreed piloting requirements as set out in DE4A deliverables, including but not limited to architectural requirements and the use of reference code.

Where a signatory feels that adherence to these deliverables is not feasible or unsuitable for a piloting activity in which they are engaged, they will endeavour to share this concern with other parties involved in that piloting activity as soon as reasonably feasible, and at any rate prior to initiating the piloting activity.

Where a signatory feels that the requirements of a deliverable are inadequate or unfeasible or unsuitable for a piloting activity in which they are engaged, they will endeavour to share this concern with other parties involved in that piloting activity, and with the DE4A partner who is the lead responsible for that deliverable, as soon as reasonably feasible. They will seek in good faith to agree on clarifications or amendments to that deliverable, and to communicate these to other affected parties.

8.2.3 In relation to piloting

The DE4A project will likely engage in a broad spectrum of piloting activities. These can include :

- activities that involve solely fictitious data and fictitious evidence, exchanged in fake procedures running in test environments; or
- activities undertaken in testing and pre-production environments requiring higher assurances that involve real-life data with real-life evidences, exchanged in actual procedures running in operational environments, with persons having prior knowledge of the DE4A project; or
- activities requiring higher assurances that involve real-life data with real-life evidences, exchanged in actual procedures running in operational environments, with persons (citizens or businesses) who have no particular fore-knowledge of the DE4A project.

The signatories agree that a nuanced approach is warranted, so that more flexibility is possible in low-risk piloting activities, and higher assurances are available in high-risk piloting activities.

Furthermore, the signatories agree that this MoU will govern the piloting activities of all signatories, irrespective of whether the piloting activities would fall within the scope of the SDGR.

8.3 Piloting in DE4A

8.3.1 Pilot types

This MoU considers three types of piloting activities:

- 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.

For the purposes of this MoU:

- Fictitious persons are natural or legal entities which do not exist in real life. The persons are made up for testing purposes (although they should appear credible and some of their characteristics (e.g. their names) could theoretically correspond to real-life persons).
- Fictitious data is any data (including any evidence) that has been generated for testing purposes in relation to a fictitious person. Fictitious data should appear credible and could theoretically correspond to real-life data, but has not been copied from real-life data.
- Test procedures are any administrative procedures that are clearly distinguishable as such by all parties involved in the piloting activities, and which run exclusively on non-production environments - i.e. they cannot result in any legal effects or practical impacts on any real-life persons.
- Real-life persons are natural or legal entities which exist in real life.
- Real-life data is any data (including any evidence) relating to a real-life person.
- Production environments are any ICT systems (or components thereof) which are used by a competent authority for real-life procedures, i.e. procedures that can result in legal effects or practical impacts for real-life persons, or that can impact the accuracy or integrity of the data and databases held by competent authorities involved in the procedures.

In low-risk piloting activities, virtually no constraints (i.e. technical, legal and organisational measures limiting the impact of the activities on the fundamental rights and freedoms of real persons) must be applied, since no negative impacts can realistically occur in relation to real-life persons, procedures or systems.

In medium-risk piloting activities, some constraints should apply as will be explained below, since some negative impacts can occur in relation to real-life persons, procedures or systems.

In high-risk piloting activities, it is advisable under this MoU to apply more significant constraints as will be explained below , since significant negative impacts can occur in relation to real-life persons, procedures or systems.

Note that, purely by way of examples, as other situation may arise during the piloting:

- Any procedures involving real-life persons are automatically considered as at least medium risk (even e.g. if fake evidence is used, and even when running only on pre-production environments). This is because real-life persons may become identified due to incidents, resulting in negative consequences that may be difficult to manage (e.g. a real-life person is incorrectly revealed to receive a (fake) pension from another country in a (fake) procedure – the fakeness may not be readily apparent to external persons).

- Any procedures running on production environments are similarly considered to be at least medium risk, since an incident may impact the environment (which is by definition used for real life procedures), even if no real-life person or data is involved.

8.3.2 Shared principles in relation to all piloting activities, including communication within the DE4A Consortium

Any piloting activity in the scope of this MoU involves at least two signatories.

The signatories declare their mutual understanding that, prior to initiating any piloting activity, they endeavour to agree in writing on the risk qualification (low risk, medium risk, high risk) that applies to their piloting activity.

They may choose to make this qualification as broad or as fine grained as seems suitable to them (e.g. by applying a different qualification depending on the use case or iteration), provided that it is clear to the participants in each piloting activity which risk qualification applies, and why (e.g. because it involves real life persons, real life data, production environments, etc).

The signatories agree that the qualification is determined by the most elevated risk in the piloting activity. E.g. if one party uses a test environment in a piloting activity but the other uses a production environment, the production environment determines the risk qualification.

The signatories furthermore agree that the qualification is dynamic, and that the progression of the pilot may result in risk profiles being elevated (e.g. a low risk activity becomes medium risk because real life data is now being used) or being lowered (e.g. a high risk activity becomes medium risk because the participants decide no longer to use production environments for future piloting). They endeavour to keep each other informed of such changes in good faith.

The signatories agree to communicate in good faith between each other on any incident or development that affects the risk qualification of their piloting activities, using the governance structure elaborated per pilot (as described in the three Pilot Planning deliverables D4.2, D4.6, and D4.10) [15][16][17]. They furthermore agree to communicate relevant information to other pilot participants in their piloting activities through this structure, in cased of any noncompliance with this MoU that may affect other pilot participants.

8.3.3 Low risk piloting

The signatories affirm their mutual understanding that low risk piloting implies no specific constraints or obligations on any side (other than the good faith communication set out in 8.3.2,) given the inherent lack of potential impact on persons, data or systems.

8.3.4 Medium risk piloting

The signatories affirm their mutual understanding that medium risk piloting should involve:

- An active communication to any real-life person (if applicable) informing them of the fact that they are involved in piloting activities, including the identification of any risks and countermeasures taken, and the (lack of) legal effects and consequences of participation. The communication should be done in their own language, in an accessible manner, and providing usable contact information. If the GDPR applies, such information provision should satisfy the requirements of the GDPR. Appropriate documentation should be retained to demonstrate that this information has been provided.
- If the piloting involves real-life persons, piloting should be organised under the supervision of a DPO.
- If the piloting would be done on a production environment, all pilot partners should notify any operators of such environments in their respective countries in advance, and appropriate measures

should be taken that piloting activities do not result in negative legal or practical consequences for any real-life persons, real life data, or production environments10. The production environments should be cleaned if the piloting activity was not intended to have long term legal or practical consequences for any real-life persons, real life data, or production environments, even after project termination.

- 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) in a manner that allows any incidents to be detected and remedied (including by contacting any affected real-life persons where needed).

8.3.5 High risk piloting

The signatories affirm their mutual understanding that high risk piloting should involve:

- All measures that apply to medium risk piloting as set out in 8.3.4
- The DE4A project DPO 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.
- The implementation of a pilot monitoring and remediation strategy as a part of the governance structure elaborated per pilot (as described in the three Pilot Planning deliverables D4.2, D4.6, and D4.10) [15][16][17], covering all participating countries, to assess whether exchanged evidences are reasonably capable of satisfying the legal, technical and operational requirements for high risk piloting, including in terms of data quality, 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 for any real-life persons, real life data, or production environments.

8.4 Statement of endorsement

On behalf of [*identification of the legal entity involved in a piloting activity – name, legal form, address – should be identical to the Grant Agreement/Consortium Agreement if applicable*],

[*Name*], [*Function*]

Hereby declares that the aforementioned entity intends in good faith to adhere to the terms of the Memorandum of Understanding in relation to its piloting activities in the DE4A project.

[*Date*] [*Location*] [*Signature and/or stamp*]

[10] By way of non-exhaustive examples, one might consider the automatic discarding of cross-border evidence received through the DE4A technical system after the submission step, preventing it to be definitively entered into the requesting competent authority's system; or marking such data in a way that makes it easier for the data to be identified and deleted afterwards if this is needed. Alternative measures include active and live monitoring of logs to comprehensively track any changes in affected systems, or the intervention of pilot stewards at each piloting entity who can ensure that incidents are monitored and addressed appropriately, and who communicate between each other to flag and address any issues that emerge.

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, 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

[13] DE4A Consortium, D2.1 Architecture Framework

[14] DE4A Consortium, D2.4 Project Start Architecture (PSA)

[15] DE4A Consortium D4.2 Studying Abroad - Pilot Planning

[16] DE4A Consortium D4.6 Doing Business Abroad - Pilot Planning

[17] DE4A Consortium D4.10 Moving Abroad - Pilot Planning

[18] DE4A Consortium Description of the Action (DoA)