

D7.1 Overview of legal and ethical requirements

|  |  |  |  |
| --- | --- | --- | --- |
| Document Identification | | | |
| Status | Draft | Due Date | 31/08/2020 |
| Version | 1.1 | Submission Date | 31/08/2020 |

|  |  |  |  |
| --- | --- | --- | --- |
| Related WP | WP7 | Document Reference | D7.1 |
| Related Deliverable(s) | WP4, WP7, WP8, WP9 | Dissemination Level (\*) | CO |
| Lead Participant | Timelex | Lead Author | Hans Graux, Mahault Piéchaud Boura (Timelex) |
| Contributors | Name (PartnerName); Name (PartnerName) | Reviewers | Ivar Vennekens and Ard van der Heijden (RVO); |
| Ana Rosa Guzmán Carbonell (MPTFP-SGAD); |

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

Document Information

|  |  |
| --- | --- |
| List of Contributors | |
| Name | Partner |
| Hans Graux | Timelex |
| Mahault Piéchaud Boura | Timelex |

|  |  |  |  |
| --- | --- | --- | --- |
| Document History | | | |
| Version | Date | Change editors | Changes |
| 0.1 | 31/07/2020 | Mahault Piéchaud Boura | Initial version of document |
| 0.5 | 11/08/2020 | Hans Graux | First round of updates |
| 0.7 | 19/08/2020 | Hans Graux | Finalisation for internal validation |
| 1.0 | 31/08/2020 | Hans Graux and Mahault Piéchaud Boura | Final version for submission; integration of feedback from Ivar Vennekens and Ard van der Heijden (RVO); and from Ana Rosa Guzmán Carbonell (MPTFP-SGAD); |
| 1.1 | 14/03/2021 | Hans Graux and Mahault Piéchaud Boura | Update after feedback from reviewers – removing duplications from the Executive Summary, and addition of a summary table in the Conclusions section (chapter 6) on legal similarities and differences across Member States; integration of various targeted comments from Alberto Crespo, notably in relation to more recently published information |

|  |  |  |
| --- | --- | --- |
| Quality Control | | |
| Role | Who (Partner short name) | Approval Date |
| Deliverable leader | Hans Graux (Timelex) | 31/08/2020 |
| Quality manager | Julia Wells (ATOS) | 31/08/2020 |
| Project Coordinator | Ana Piñuela Marcos (ATOS) | 31/08/2020 |

Table of Contents

[31/08/2020 1](#_Toc66660125)

[Document Information 2](#_Toc66660126)

[Table of Contents 3](#_Toc66660127)

[List of Tables 5](#_Toc66660128)

[List of Figures 6](#_Toc66660129)

[List of Acronyms 7](#_Toc66660130)

[Executive Summary 8](#_Toc66660131)

[1 Introduction 9](#_Toc66660132)

[1.1 Purpose of the document 9](#_Toc66660133)

[1.2 Structure of the document 10](#_Toc66660134)

[2 General outline of the requirements set in the SDGR 11](#_Toc66660135)

[2.1 The SDGR’s perspective on the OOP and Article 14 11](#_Toc66660136)

[2.2 Requirements for the technical system under the SDGR 13](#_Toc66660137)

[2.3 OOP, DE4A and e-government beyond the SDGR 13](#_Toc66660138)

[3 Critical legal issues in DE4A 15](#_Toc66660139)

[3.1 Preview of evidence exchanged 15](#_Toc66660140)

[3.1.1 Introduction – the role of the preview in the SDGR 15](#_Toc66660141)

[3.1.2 Implications of this understanding – implementing a preview functionality 17](#_Toc66660142)

[3.2 Explicit request, including in relation to consent and the preview obligation 23](#_Toc66660143)

[3.2.1 Introduction – the role of the explicit request in the SDGR 23](#_Toc66660144)

[3.2.2 Implications of this understanding – implementing an explicit request functionality 27](#_Toc66660145)

[3.3 Data subject rights in the context of the SDG 29](#_Toc66660146)

[3.3.1 Introduction – Data subject rights in the GDPR, and relationship to the SDGR 29](#_Toc66660147)

[3.3.2 Data controllers and data subject rights in the SDGR 33](#_Toc66660148)

[3.3.3 Implementing data subject rights in the context of the SDGR and the technical system 34](#_Toc66660149)

[3.4 Structured versus unstructured data in the context of the SDGR 37](#_Toc66660150)

[3.4.1 Introduction – Evidence in the SDGR and the concept of structured data 37](#_Toc66660151)

[3.4.2 The SDGR and its “electronic format that allows automated exchange” 40](#_Toc66660152)

[3.5 Charging for evidences under the SDGR 43](#_Toc66660153)

[3.6 Further processing of evidences 44](#_Toc66660154)

[3.6.1 Further processing under the GDPR 44](#_Toc66660155)

[3.6.2 Further processing under the SDGR 45](#_Toc66660156)

[3.7 Lawfulness / legal basis of piloting prior to the entry into application of the SDGR 46](#_Toc66660157)

[4 Preliminary ethics assessment 48](#_Toc66660158)

[4.1 Provisional note on the scoping and impact of ethics under DE4A 48](#_Toc66660159)

[4.2 Measures taken 49](#_Toc66660160)

[4.2.1 Appointment of a DPO 49](#_Toc66660161)

[4.2.2 Information and consent scheme 49](#_Toc66660162)

[4.2.3 Further processing issues 50](#_Toc66660163)

[5 Data flow assessment and national or pilot specific requirements 52](#_Toc66660164)

[5.1 Relevance of the preliminary data flow assessment 52](#_Toc66660165)

[5.2 General DE4A approach and working assumptions in relation to responsibilities 52](#_Toc66660166)

[5.3 National or pilot scenarios specificities 54](#_Toc66660167)

[5.3.1 Studying abroad 54](#_Toc66660168)

[5.3.2 Doing Business Abroad 55](#_Toc66660169)

[5.3.3 Moving Abroad 55](#_Toc66660170)

[6 Conclusions 57](#_Toc66660171)

[References 60](#_Toc66660172)

List of Tables

[Table 1 : Rights available depending on the legal basis 33](#_Toc66659852)

[Table 2 : Categories of personal data used in the Studying abroad pilot 55](#_Toc66659853)

[Table 3: Categories of personal data processed in the Moving Abroad pilot 55](#_Toc66659854)

[Table 4: Legal conclusions on system requirements 58](#_Toc66659855)

[Table 5: Similarities and differences between the Member States 59](#_Toc66659856)

List of Figures

[Figure 1: Illustration of fluidity of the concept of "evidence" 36](#_Toc49176995)

[Figure 2: Primary intermediation pattern, see D2.1 50](#_Toc49176996)

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 |
| 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 |
| 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/> |
| ZKP | Zero Knowledge Proof |

Executive Summary

This deliverable is the first formal output of WP7 (Legal and ethical compliance and consensus building) for the DE4A project, and aims to provide an initial identification and assessment of legal and ethics challenges for the project and its piloting activities.

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 currently ongoing between Member States, and towards the European Commission, on the exact interpretation and intended impact of the SDGR. Since these discussions are far from concluded, it is clear that the legal findings of this deliverable are largely tentative and subject to evolution.

None the less, this report aims to present the central topics that have been under discussion within the consortium, and captures some of the main positions taken on the meaning of the SDGR at the time of submission. More importantly, it summarises the working assumptions on the interpretation and impact of the law on the project. In other words, it is not an abstract reflection on legal difficulties, but lays out what the consequences of specific interpretations would be, and which interpretations the consortium intends to apply during piloting.

Key topics covered by this deliverable include the preview requirement, explicit request, GDPR compliance, the relevance of structure in exchanged evidences, charging, lawfulness of piloting and further processing of evidences. These topics are developed iteratively and interactively through white papers and online discussions between all project partners. In this way, the positions taken in this deliverable may not necessarily be conclusive, but they will be informed and driven by existing understanding of the law across DE4A members.

As the report will show, there are many uncertainties still on the exact interpretation of the SDGR. It is intended that the findings of this report and its working assumptions will be further refined and adjusted, based on future discussions and working experiences in DE4A. In this way, they can contribute further to achieving consensus between the Member States, and in providing useful feedback to national and EU level legislators and policy makers, so that the SDGR can achieve its intended goals.

# Introduction

## Purpose of the document

The present document is the first 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:

1. Continued assessment of existing and emerging legal requirements
2. Assisting the translation of such legal requirements into technical, operational or infrastructural requirements
3. Building consensus on best practices in compliance
4. 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 first deliverable in WP7, identifies and scopes legal and ethical requirements for the execution of the pilots at an early stage in the project. These result principally from EU level legal restrictions – notably those resulting from the SDGR (such as the prior request or the preview functionality), but also from the GDPR (such as the need for lawfulness, proportionality and privacy by design), and legislation such as the eIDAS Regulation that underpins some of the components (eID, eSignatures, eSeals and so forth) that will support the project’s execution.

However, national constraints need to be identified as well, both to determine pilot specific possibilities (e.g. no request or preview is required under the SDGR if national legal frameworks permit exchanges of evidence without a request or preview) and to determine pilot or Member State specific constraints (e.g. requirements to obtain authorisations from a national supervisor, or to conclude prior agreements to scope exchanges of evidences).

This document captures the current understanding of legal and ethics requirements at an early stage of the project, and current working assumptions notably in relation to architecture and pilot execution.

It is worth stressing that the interpretations in this document are highly subject to evolution, both due to ongoing discussions on exact pilot scoping and approach, and due to the discussions between the Member States and the European Commission on the implications of the SDGR and its further implementation. As a result, D7.1 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 matures.

## 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
* Chapter 3 – Critical legal issues. This chapter outlines the main legal issues that have been assessed during the first 8 months of the DE4A project, and contains a summary of current understanding and working assumptions
* Chapter 4 – Preliminary ethics assessment. This chapter examines the main ethics challenges in DE4A, and outlines the measures already taken.
* Chapter 5 – Data flow assessment and national/pilot specific requirements. This chapter summarises general data flows, as a building block to determine pilot specific issues. This will be elaborated further once details of the pilots are more clearly fixed.
* Charter 6 – Conclusions. This chapter outlines the main findings, and lists next steps in WP7.

# General outline of the requirements set in the SDGR

The general objective of this deliverable is to identify and assess legal and ethics requirements in DE4A. 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.

The purpose of this first section of the deliverable is therefore to identify and assess the legal requirements set forth in the SDGR, and to describe the impacts and potential constraints on DE4A. The analysis of critical legal issues will be expanded in Chapter 3.

## 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]](#footnote-1), the Directive  on services in the internal market[[2]](#footnote-2), the Directive on public procurement[[3]](#footnote-3), and the Directive on procurement by entities operating in the water, energy, transport and postal services sectors[[4]](#footnote-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 transfer of evidence;
* It must enable requesting evidence,
* It must allow  the transmission of 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 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.

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 they prefer, and provide the evidence in an alternative manner. Moreover, the use of the technical system must be ‘explicitly requested’ by the user; it cannot be the default mode of transfer of evidence. 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. 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. This approach has implications for some piloting scenarios, as will be further discussed in the sections below.

## Requirements for the technical system under the SDGR

Article 14 sets out several general legal requirements for the technical system. 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 allowed 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.

## OOP, 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, notably because its piloting applications largely fall within the scope of the SDG online procedures.

However, 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. The principal 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. It is understood that these are unlikely to fall entirely within the boundaries of the SDGR, and therefore that piloting with real-life cases and real-life data will not have a clear legal basis in the SDGR. None the less, with a view to evolving towards optimal e-government services, the DE4A project will continue to evaluate these alternative scenarios, and may choose to pilot them in the future, to the extent that this can be lawfully done. This issue will be actively monitored and reported upon in future WP7 deliverables.

# Critical legal issues in DE4A

Task 7.1 aims to identify and scope the legal and ethical requirements for the development of the DE4A solution and the execution of the pilots. These general (non-pilot specific) requirements at the EU level have been identified based on the analysis of the SDGR, GDPR, and in discussion with the partners; national or pilot specific requirements will be briefly discussed in Chapter 5 below.

Methodologically, the list of critical legal issues is maintained in dialogue with all project partners, where new issues can be added upon request. At the time of submission of this deliverable, the following topics have been discussed at some length already:

* The preview requirement of Article 14
* The explicit request requirement of Article 14
* GDPR data subject rights in relation to once-only exchanges
* Requirements on the structure of exchanged evidences

In addition, preliminary analysis has been done in relation to the legal basis for piloting activities, further processing of evidence after the exchange, and charging for evidence under the SDGR. The current state of play on these topics will be summarised in this deliverable. As already highlighted above, the deliverable captures only the current understanding, which is subject to significant further evolution as discussions between the Member States and with the European Commission on the interpretation, application and implementation of the SDG evolve.

## Preview of evidence exchanged

### Introduction – the role of the preview in the SDGR

#### Context – Once-only in the SDGR, and the principle of a preview in the SDGR

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.

For the avoidance of doubt, it should be noted that the preview requirement is separate from the explicit request requirement. It is possible for a procedure to require a request but not a preview, or the other way around (and neither the preview nor the request are equivalent to a ‘consent’ under the GDPR, as will be explored in the section on consent/request below). For this reason, it would not be recommended to implement the preview as a single integrated module which is intrinsically combined with the request in the user interface: there can be cases where only one of both requirements applies.

#### What is the general purpose of a preview?

The preview mechanism aims to support the accuracy and relevance of the data exchanged and strengthens control by the user over data exchanged through the technical system, allowing them to exercise some control over the consequences of their use of the system.

Recital 47 of the SDGR indicates that the use of the technical system should be voluntary, and other means of submitting evidence should remain available to users. The recital further explains that the user *“should have the possibility to preview the evidence and the right to choose not to proceed with the exchange of evidence in cases where the user, after previewing the evidence to be exchanged, discovers that the information is inaccurate, out-of-date, or goes beyond what is necessary for the procedure in question. The data included in the preview should not be stored longer than is technically necessary.”*

Although the recital reinforces the notion of user control of the information exchanged, it also suggests that the preview is a means to support compliance with several data protection principles stated in the GDPR, notably data minimisation (data should be processed only to the extent necessary to achieve the purpose sought), accuracy (the data should be as correct and up to date as possible) and transparency (data subjects should clearly understand that personal data concerning them is processed, to what extent and for what purpose)[[5]](#footnote-5). The integration of these principles in the technical system envisaged by the SDGR can be considered an application of the privacy by design principle.

#### Understanding the general goals - what are the interactions between the preview mechanism and data protection principles?

While not all evidences exchanged via the technical system will be by definition qualified as personal data, it seems clear, given the text of the recital, that the preview mechanism at least to some extent helps to support compliance with key data protection principles, in particular transparency, data minimisation and data accuracy.

Indeed, the preview mechanism provides a direct opportunity for the user (either a natural person, or a legal person represented by a natural person in a specific exchange) to literally see the data to be exchanged relating to them. The mechanism in that regard is a good enabling factor for the exercise of the rights of the data subjects. It grants *de facto* the right to access the data and can support the rights of restriction of processing and the right to object to the processing (by aborting an exchange of evidences after the preview). Of course, if a user exercises this right by refusing to approve an exchange after seeing a preview, the procedure will in principle be aborted, since the competent authority will not receive evidence that it indicated as being necessary.

However, the implementation of the preview mechanism also raises data protection questions. Exchanging information concerning the user through the technical system will result in the processing of personal data as understood in the GDPR. It must therefore be compliant with the GDPR principles. In particular, the principle of data minimisation[[6]](#footnote-6) creates two specific challenges.

Firstly, in principle, processing of personal data must be limited to what is absolutely necessary for the purposes, i.e. the evidence provided should be limited to what is necessary for the procedure at hand. Ideally, this would imply the exchange (or at least the use) only of assertions in relation to the user, rather than of entire documents that would likely contain more information than needed, but it is doubtful that this can be achieved in many piloting use cases. Likely, the default situation will be that the exchanged evidence will contain more information than is strictly required because of the fact that these documents are standardised in a manner which is not dependent on foreign procedural requirements, and the main obligation for the consuming authority is to process the information from the evidence only insofar as this is necessary for the completion of the procedure at hand. This issue will be examined further in the section on structured data.

Second, because data minimisation is also generally understood as the minimisation of the instances where personal data is processed, the timing of the preview (or more practically: the location of the data at the time of the preview) is crucial. If the preview only occurs *after* the transfer of the evidence to the consuming authority, the evidence may be subjected to more processing – and certainly to more exposure - than can be justified.

The main implications of these issues will be examined below.

### Implications of this understanding – implementing a preview functionality

#### When and where should the preview occur?

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”.

Given this phrasing and the data minimisation logic as outlined above, from a legal perspective it is preferred that **the preview possibility is offered to the user *before* the exchange to the consuming authority occurs**. A broader interpretation, where the consuming authority first receives the evidence and then allows the user to preview it and to block any use of the data, arguably raises compliance challenges with the phrasing of the SDGR: the SDGR requires that the user can preview the evidence *and* choose whether to proceed with the exchange, suggesting that an exchange followed by a preview is not in line with legal requirements. It is also somewhat at odds with the GDPR, since a preview after the exchange implies processing (exposure to the consuming authority) of personal data that could have been avoided and which is not technically necessary for the technical system to function, and therefore would be an implementation that creates needless data protection risks. Therefore, from a strictly legal perspective, the preview should ideally take place before the evidence is transferred to the competent authority in the destination Member State.

However, the SDGR is not unambiguous on this point. The phrasing of the preview principle contains no temporal component: the user must be able to preview *and* decide to proceed with the exchange; not to preview *before* deciding to proceed. An approach where the user decides whether to proceed with an exchange and is given the possibility to preview afterwards is perhaps counterintuitive and less in line with privacy by design, but not formally contrary to the requirements of the SDGR.

From that perspective, the current architectural model of DE4A offers some opportunities for nuance. Specifically, it makes an explicit distinction at the data consumer side between the **Data Evaluator** and the **Data Requestor**. The Data Evaluator is any organization authorized to receive and process data from the user, whereas the Data Requestor is the role which enables search and request functionalities from a technological perspective. In simpler terms, the Evaluator is the entity which is required to receive and interpret the evidence in order to complete the procedures, and the Requestor merely is tasked with finding and providing that evidence to the Evaluator.

Where these roles are allocated to two different entities (i.e. the Requestor is an entity that locates the evidence for a specific and separate Evaluator entity), it is possible to allow the preview to be provided by the Requestor, without also providing the evidence to the Evaluator. This would seem to mitigate the SDGR and GDPR challenges: the evidence can be previewed (with the Requestor) before proceeding with any exchange to the competent authority (the Evaluator), as the SDGR requires; and personal data processing is less invasive (given the smaller exposure) than organising the preview at the Evaluator’s side. In other words, while a technical exchange of the evidence already happens before the preview, no use is made of the evidence other than enabling a preview until the user has decided to proceed. Given that, as noted above, the phrasing of the SDGR has no temporal component, and that this approach mitigates data protection and confidentiality risks to some extent, it can be seen as a reasonable balance.

The approach might also be seen to have some support in the current interpretation of the SDGR by the European Commission. The European Commission – DG GROW published the following question and answer on the SDG Wiki[[7]](#footnote-7):

***11. What else is requested for the once only technical system to be compliant with the GDPR?***

*The SDGR clarifies the three requirements in order for the system to be compliant with the GDPR:*

* *That the exchange is initiated at the request of the user, unless provided otherwise under Union or national law – this explicit request is the tool that will be used to demonstrate consent of the user*
* *That the user can preview the evidence before it is used by the authority that needs it*
* *That the evidence is used only for the purpose for which it was exchanged.*

*The legislator considered these three requirements to be sufficient to ensure compliance of the OOP system with the GDPR.*

It is worth noting that the phrasing of the preview requirement in the FAQ – *that the user can preview the evidence before it is used by the authority that needs it* – is perfectly aligned with the roles explained above. As a non-legal consideration, the approach is also significantly more user friendly and technically more robust in scenarios where evidences must be obtained from multiple sources in potentially multiple Member States: a requirement to enable the preview at each different source creates multiple points of failure and multiple preview steps, and also results in linguistic challenges when each evidence source should present previews to users across the EU; whereas a transfer of the evidences followed by a single preview at the recipient’s side eliminates these to some extent.

A comparable nuance is also added at the data provider’s side in the current DE4A architectural model, where the data providing roles are split into the **Data Owner** (entity holding the evidence) and the **Data Transferor** (the role which bundles evidences and sends them to the Data Requestor).

**Taking these elements into account, four implementation options** seem to be conceptually possible for the timing of the preview:

1. **Preview with the data provider Member State**: The evidence is collected in the issuing authority’s Member State and shown to the user via components of the architecture under the control of that Member State. This could be implemented either by requiring the **Data Owner** to show a preview, or by allocating this task to a **Data Transferor** (e.g. by having a ‘national node’ that implements the preview functionality, thus saving all issuing authorities from implementing and maintaining these components individually). The user then decides whether the evidence should be transferred to the technical system. **This seems clearly compliant with the SDGR and GDPR.**
2. **Preview with the data consuming Member State**: The evidence is collected in the data providing Member State(s) and transferred to components of the architecture under the control of the Member State of the Data Evaluator. This could be implemented either by requiring the **Data Evaluator** to show a preview, or by allocating this task to a **Data Requestor**. As argued above, having the **preview done at the Data Evaluator’s side** seems contentious, since this implies that the exchange to the consuming authority is technically done before the user can indicate whether they wish to proceed with that exchange**.** It also creates needless risks under the GDPR, since it implies that personal data is processed by the Data Owner, Data Transferor (if any), Data Requestor (if any), *and* Data Evaluator before the user can decide on the legitimacy of the exchange. It could of course be assumed that the Data Evaluator will act in good faith and refrain from any other use than previewing the evidence until the user decides to proceed, but if this was the intended outcome, it is not clear why the SDGR would phrase the preview and approval requirement as deciding to “proceed with the exchange”, rather than “proceed with the use”.

Alternatively, the **preview could also be done at the Data Requestor’s side.** This seems more easily defensible, since the consuming authority receives no evidence until the user can indicate whether they wish to proceed with the exchange. This seems **in line** **with the SDGR.** The data protection risks are also more easily manageable: while the data is still exposed to a Data Requestor (implying cross-border transfer of personal data prior to any preview), the personal data can be shielded from any use other than previews, which seems an acceptable proposition.

1. **Preview with the user**: The evidence is collected in the data provider’s Member State and transferred to components of the architecture under the control of the user itself (i.e. a secure storage box accessed through its browser, a secured app, other software,…). The user then decides whether the evidence should be transferred to the competent authority. This can be considered a ‘personal vault’ based approach, with the user controlling their own vault and its use. This seems **compliant with the GDPR**, and can be seen as strongly empowering the user, supporting its data subject rights and the data portability objectives of the GDPR.

However, there are also some weaknesses. Firstly, care should be taken that **this approach is not implemented in a way that undercuts the once-only principle as envisaged by article 14**: the objective of the SDGR is that the evidence is transferred from one authority to another. A user controlled vault should not result in the user being made responsible for identifying next steps in a process, finding parties to correspond with, fixing problems in an exchange, etc.

Secondly, there is a conceptual risk: if the user indeed has full control over their vault, this could also imply that the user could transfer the evidences to any desired recipients, not just authorities. Member States and authorities would lose control over the usage of the evidences. Effectively, this would make the SDGR and the vault a tool for accessing governmental information (possibly undercutting national laws on access to public sector information or freedom of information requests), and even for circumventing laws on re-use of public sector information (as harmonised at the EU level through the Open Data Directive). There is thus a risk to this approach that seems hard to mitigate, unless stringent constraints are applied to the vault to ensure that the data can only be transferred to a competent authority in another Member State.

1. **Preview with the central SDG**: The evidence is collected in the data provider’s Member State and transferred to centralised components of the technical system, which is under the control of the Commission (i.e. the single digital gateway on the Your Europe portal, and/or its common user interface as described by the SDGR). The user then decides whether the evidence should be transferred to the competent authority. This seems **suboptimal both under the SDGR and the GDPR,** since it implies exposure of the evidence to a party (the Commission) that does not need to receive it, and since it arguably is not a function entrusted to the Commission under the SDGR.

Given the purpose of the preview mechanism and the principles behind the SDGR and the GDPR, from a legal perspective the preferred approaches are option 1 (**Preview with the data providing Member State),** with defensible alternatives being option 2 (**Preview with the data consuming Member State, through the Data Requestor**) and option 3 (**Preview with the user)** if appropriate safeguards are implemented that can minimise abuse risks. Preview at the Data Evaluator’s side seems legally non-preferred, since it suggests avoidable risks: in the event where the user decides not to exchange the evidence, or indicates that corrections are necessary, the exchange has already occurred. Avoiding unnecessary exchanges of evidence is a matter of data protection by design and by default, which is required by the GDPR.

The principal challenge in interpreting the SDGR’s phrasing on previews thus relates to the temporal aspect (when must it take place?) and to the distinction between exchange of the evidence and use of the evidence. The SDGR states that the user must have the possibility “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”. This paper interprets the first part of that statement as scoping (“the evidence to be used by the competent authority”), and the second part as the preview rule (“choose whether or not to proceed with the exchange”), thus concluding that the exchange may not take place until the preview is done.

It is however also possible to read these two phrases as more closely intertwined, arguing that one may proceed with the exchange provided that no use is made of the evidence other than the preview – i.e. this is a more functional approach which recognises that the principal risk is precisely that evidence is used for other purposes than the preview, and that the SDGR is complied with as long as such uses are avoided. Under that reading, one might also argue that a preview can be done anywhere, including by the Data Evaluator (and therefore *after* the exchange), as long as the Data Evaluator doesn’t use the evidence until the preview has been done and the exchanged has received the approval of the user. Currently, this deliverable does not fully adopt this logic, but the DE4A consortium will continue to engage in dialogues with various stakeholders in order to determine whether it may also be viable.

**In conclusion, the paper presently adopts the working assumption that previews can be lawfully organised with the data providing Member State (either the Data Owner or the Data Transferor), or** **with the data consuming Member State through the Data Requestor**, **or with the user. Any of these scenarios may be piloted in DE4A.**

In practice, current discussions would suggest that previews at the Data Requestor role may be more viable in practice, since organising the preview at the data providing Member State implies extremely complex data flows which create information security risks, decrease user friendliness, introduce language and accessibility challenges, and strongly reduce the robustness of the system. These technical and functional downsides to some extent negate the conceptual data protection and confidentiality benefits of a preview at the data providing Member State’s side. Furthermore, scenarios where evidences are collected from multiple organisations in multiple Member States rapidly become extremely user unfriendly if previews indeed have to be organised at the (multiple) Data Owners or at the (multiple) Data Transferors.

#### Preview as a ‘possibility’ when using the technical system

The preview mechanism must be built into the architecture, but this does not imply that it will or must be used for every cross-border exchange of evidence. Firstly, it is worth noting that the use of the technical system for exchanging evidences is not mandatory under the SGDR. Evidence may only be exchanged through the technical system at the ‘explicit request’ of the user, unless it is required by EU or national legislation; and users are permitted to submit evidence by means other than the technical system and directly to the requesting competent authority (article 14.4 SDGR).

Secondly, the provision on previews notes explicitly that the technical system must ‘enable the possibility for the user to preview the evidence’. It is not mandatory for previews to be shown by default. It would therefore seem acceptable to implement a preview functionality which is only activated after the user explicitly requests it (“Click here if you wish to preview the evidence that will be transferred in the course of this process”); this is also increases user friendliness by allowing users to avoid the preview step if they deem it unnecessary (e.g. when they have full confidence in the accuracy of the evidence on the basis of their prior experience). This creates the possibility of building the preview functionality at the data providing Member State’s side, even without any harmonisation between Member States (other than the requirement that the functionality should exist and be available to users, and that users should be able to abort a transfer of evidences after seeing the preview).

#### What are the exceptions to the preview obligation, and how can this be implemented?

The SDGR indicates that the possibility of a preview is not required when “automated cross-border data exchange without such preview is allowed under applicable Union or national law” (14.5 SDGR). Experiences in the course of the DE4A project may change our understanding of this principle, but at present there are no known instances (and nor are they likely to exist) of national or EU level laws that explicitly reference a ‘preview’ before exchanging information. As a result, this exception likely applies mainly to:

* Evidences which are **publicly available to anyone without any constraints** (e.g. via public websites, open web services, etc.). In such cases, it seems reasonable to argue that automated cross-border exchange without preview is allowed.
* Evidences which are **available to designated competent authorities within the EU** (without constraint to one or several specific Member States). Based on initial discussions, social security documents that can be exchanged via the EESSI network seem to be an example, since the EESSI legislation allows competent authorities to exchange information directly in the circumstances covered by that legislation (without preview by the user). In such cases it seems reasonable to argue that automated cross-border exchange without preview is allowed.

If this understanding proves to be correct, and if DE4A chooses to implement an infrastructure that can also identify and respect the exception to the preview question, then this also has architectural implications. Mainly:

* **Competent authorities should be able to query for each Member State a catalogue of types of evidences available to anyone without any constraints, which should be maintained and made available via the technical system.** If an exchange of such evidences is requested, the technical system should be able to detect it via this database and may omit the preview possibility. The database can of course be blank if a Member State considers that none of the supported evidences are publicly available to anyone without any constraints.
* **Competent authorities should be able to query for each Member State a catalogue indicating, on a per use-case basis, whether the relevant evidences can be exchanged to specific competent authorities in other Member States.** Again, if an exchange of such evidences in the relevant use case is requested, the technical system should be able to detect it via this database and may omit the preview possibility.

Member States could of course also simply choose always to offer the preview possibility (even in cases where this may not be legally necessary), in which case the architectural implications above could be ignored (or at least they could remain un-implemented in DE4A).

One additional complexity is the issue of which ‘national law’ determines whether a preview can be omitted or not. The explanation above assumes that the main relevant question is whether the evidence is publicly available without constraints – and therefore that only the national laws of the data providing Member State govern the preview exception. However, a much stricter interpretation could be applied as well, in which the omission of a preview is governed by any national laws determining the rules behind a specific procedure. In that interpretation, the national laws of the data consuming Member State are equally relevant – i.e. if an evidence is freely available in Member State A, but Member State B does not recognise the free availability of that type of evidences in a specific procedure, Member State B might insist on previews, arguing that its own laws are not complied with if no preview was available. This is an open issue at present.

#### Duration of storage

Finally, recital (47) of the SDGR also indicates that “the data included in the preview should not be stored longer than is technically necessary”. Given the reference to technical necessity, this constraint seems to target only the storage required for the preview functionality, and not any storage that precedes or follows the preview (e.g. retention in the sending Member State for accountability purposes, or retention in the receiving Member State for the purposes of administrative follow-up of the service requested by the user).

In addition, the reference to “data included in the preview” seems to suggest that it is principally the evidence’s content that may not be retained longer than necessary, which is reasonable from a data protection and confidentiality perspective. No part of this provision would seem to suggest that an audit trial is impermissible, provided that the audit trail doesn’t include the “data included in the preview”. In other words, an audit trail could contain any metadata related to the preview process, as well as e.g. hashed values of the evidence file in order to determine afterwards (in case of disputes) whether a specific file was exchanged, provided that the evidence itself and its contents are not retained.

Based on that understanding, the main implication seems to be that the technical system must include a function that ensures that **an automated deletion of the evidence should occur after the user decides whether or not to transfer the evidence.** This deletion (from static storage devices or from dynamic memory) should be verifiable through an appropriate log or audit trail. No centralised storage of the evidence is permissible under the SDGR. This is likely an obvious requirement, except possibly if the scenario is chosen where previews are offered in the user’s own sandbox. In that case, the user may reasonably expect that the evidence actually stays in their sandbox.

This creates some tension with the SDGR, depending on how the text of the SDGR is interpreted. A strict reading would require that the user may not even choose to retain the data, since the text of the law is clear: the data included in the preview should not be stored longer than is technically necessary, and once the preview is done, no storage is technically necessary.

However, it does not seem unreasonable to argue for a more flexible interpretation, and allowing that the data of the preview may be stored if that storage is clearly communicated to the user in each transaction and they actively choose to do so (“I would like to store this document in my e-box”). In that way, longer term retention could be justified since it no longer occurs in the context of the SDGR – in other words, the deletion requirement is respected during the preview, but the user is given the right to retain data after the preview if they actively choose retention.

## Explicit request, including in relation to consent and the preview obligation

### Introduction – the role of the explicit request in the SDGR

#### Context – Once-only in the SDGR, and the principle of an explicit request in the SDGR

According to the Single Digital Gateway Regulation, 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.

The phrasing of these requirements for an explicit request is nearly identical to the definition of a ‘consent’ in the General Data Protection Regulation, which states that the “consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her” (article 4 (11)). None the less, for reasons that will be outlined below, the concepts should not be conflated: the expression ‘consent’ does not occur in the SDGR, and the notion of ‘consent’ should not be used as a reference to the explicit request requirement of article 14 of the SDGR.

Globally, from a terminological perspective, the following approach is used:

* **‘explicit request’ (or simply ‘request’)** is used as a reference to the SDGR requirement in article 14, meeting the requirements of the SDGR.
* **‘consent’** is used as a reference to the GDPR notion of a consent. This is specifically relevant when examining the legal basis for personal data processing in an evidence exchange, for which consent can be one of the options, depending on the procedure.
* **‘approval’** is used as a reference to the user’s confirmation, after a preview of evidence is shown, that the exchange of evidence may proceed (as described in 14.3 (f) SDGR: 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).

For the avoidance of doubt, it should be noted that the explicit request requirement is separate from the preview requirement. It is possible for a procedure to require a request but not a preview, or the other way around. For this reason, it would not be recommended to implement the request as a single integrated module with the preview in the user interface: there can be cases where only one of both requirements applies.

#### What is the general purpose of the explicit request?

The SDGR does not allow cross-border exchange of evidence between public authorities in all cases. Article 14 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 – exceptions will be discussed below – 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.

The inherent limitation to user-driven requests in the SDGR does not eliminate any margin of discussion on the scoping of exchanges. Specifically, one of the ambitions of the DE4A project is to pilot use cases where proactive, automated or recurring evidence exchanges can occur, which are not driven by a new request and a new preview for each individual exchange. These exchange patterns are sometimes referred to as push models (due to the fact that relevant changes in the evidence are ‘pushed’ by the evidence provider to a potentially relevant recipient, without a new request (a ‘pull’) from that recipient or from the user), or as ‘subscription’ driven models, in the sense that an interested recipient subscribes to changes in certain information, which it will thereafter receive automatically.

There is some discussion still as to whether such models could conceptually fit within the scope and approach of Article 14 of the SDGR. While these exchanges are certainly once-only implementations, they do not adhere at first sight to the central vision of the SDGR that all exchanges are driven by a user request, since subsequent exchanges could conceivably occur even without the user’s awareness, let alone without their request. None the less, this assessment is less absolute than it may seem. One might e.g. consider the case where a user explicitly requests that a certain administration obtains certain evidences for a specific procedure, and that it asks that it keeps these up to date (including through future requests) for a specified period of time. In other words, a user could request the receiving competent authority to keep the evidence up to date. There is no reason in principle that such an approach would be contrary to the SDGR’s rules on explicit request: the exchanges are indeed based on an explicit request, the scoping of which is clearly approved by the user. While each subsequent exchange (resulting from the initial request) is not the result of an entirely new request, there is no part of the SDGR’s phrasing that suggests that individual requests for individual exchanges would be necessary.

None the less, there are two major constraints that impede an easy adoption of push/subscription models as a part of Article 14 of the SDGR. Firstly, there is the consideration that the original request would at any rate need to be particularly clear and explicit on the scoping of the request, and in particular on the possibility (including purpose limitation and temporal limitation) of future exchanges. A situation where a competent authority can request evidences without limitation to specific administrative procedures or for an indeterminate period of time would not be compatible with the SDGR. Secondly, even when accepting that an explicit request can cover push/subscription models, this does not invalidate the preview requirement: the user must be able to preview each subsequent evidence exchange and be permitted to decide whether to proceed with it. This latter element inherently requires user involvement, even in push/subscription based models, which obviously removes a significant part of its utility in practice. For that reason, push/subscription based models seem hard to fit into the current model of Article 14 in a legally compliant way.

#### Understanding the relationship between the explicit request and consent under data protection law

While not all evidences exchanged via the technical system will be by definition qualified as personal data, it is clear that the explicit request requirement at least to some extent helps to support compliance with key data protection principles, in particular the requirement to have a legal basis for a transfer of evidences containing personal data.

The SDGR comments on this relationship explicitly, noting that “*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*”.

This assertion is short, but contains a few critical pointers for the interpretation of the relationship between request and consent. Notably:

* It recognises that not all evidences will include personal data. This is of course dependent on the procedure and on the evidences required. For e.g. the Doing Business Abroad pilots, evidences do not only – or often principally - concern a natural person. None the less, even there data protection law may apply, since companies often will need to provide evidences containing personal data on representatives or other stakeholders who are natural persons; in these cases, the GDPR must be complied with.
* The recital’s meaning should not be misunderstood as saying that a request is identical to consent. It notes only that, *if* evidences contain personal data *and* a consent meeting the requirement of the GDPR is obtained for the exchange, *then* the consent requirement also satisfies the requirement of the explicit request. It however does not indicate that a consent is always required, nor that every request satisfies the requirements of a consent under the GDPR.

To understand the exact relationship between the request and a consent, it is important to understand that any exchange (or other form of processing) of personal data through the technical system must comply with the requirements of the GDPR. A central challenge in any DE4A use case – among other data protection challenges – is ensuring that there is a legal basis for the transfer of evidence, assuming that the evidence indeed contains personal data. It would be tempting to assume that the explicit request of the user to transfer any personal data constitutes a consent under the GDPR, and therefore that it is sufficient as a legal basis in all cases. None the less, this would be incorrect for several reasons.

Firstly, a consent under the GDPR must be given by the data subject, i.e. the person whose data will be processed. This is sometimes not possible in specific procedures, where the user may not be the (only) person whose personal data will be processed – consider e.g. an accounting person using the SDG to transfer personal data relating to the management of a company: the accounting person cannot by definition provide consent on behalf of the management.

Secondly, consent under the GDPR must be freely given. It has been a long standing interpretation of European data protection law – and this point has been recently affirmed in official guidance from European data protection authorities[[8]](#footnote-8) – that freely given consent is not possible when there is a clear imbalance of power between the data controller (the party asking for the consent) and the data subject (the party giving their consent). The aforementioned Guidelines take a very strict approach on this point, and stress that “*it is unlikely that public authorities can rely on consent for processing as whenever the controller is a public authority, there is often a clear imbalance of power in the relationship between the controller and the data subject. It is also clear in most cases that the data subject will have no realistic alternatives to accepting the processing (terms) of this controller. The EDPB considers that there are other lawful bases that are, in principle, more appropriate to the activity of public authorities*”. While this position appears strict, it is not illogical: in the case of e.g. moving one’s home to a different Member State, there is hardly any freedom left: a citizen either consents, or is unable to move homes. In these circumstances, there is little choice in reality.

Similarly and perhaps less intuitively, the same Guidelines note that “*an imbalance of power also occurs in the employment context. Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent. Therefore, the EDPB deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees (Article 6(1)(a)) due to the nature of the relationship between employer and employee*”.

In both cases – public authorities and employees – consent is not entirely impossible if there is indeed no imbalance of power, but it is generally not the favoured legal basis for the processing of personal data under European data protection law. Where consent under the GDPR is lawfully possible, the SDGR does make it clear that the consent also satisfies the requirement of an explicit request – and a valid consent in the sense of the GDPR therefore also proves compliance with the request requirement of the SDGR.

This situation is important for some DE4A pilots, e.g. because the ‘consent’ is given within the context of a working relationship (where the user is ‘consenting’ because it is their job, and they have no real margin of choice), or there is another circumstance where the user is under such pressure from a specific hierarchy that they have no realistic alternative to ‘consenting’. In such cases, a consent meeting the requirements of the GDPR is not legally possible.

However, this is not an insurmountable problem in practice, since the GDPR does not require consent by definition, but rather a legal basis, for which consent is only one available option. The SDGR similarly does not mention consent at all – nor any other legal basis under the GDPR – thus leaving multiple justifications open. As the European Data Protection Supervisor also noted in its Opinion 8/2017 on the proposal for the SDGR[[9]](#footnote-9), “*the three most relevant legal grounds for implementing the ‘once-only’ principle are* ***consent, legal obligation and public task/official authority****. Depending on the circumstances,* ***one or another of these legal bases could be the most appropriate choice****.* ***As a general rule of thumb****, for the case of any recurring and structural data sharing, the EDPS recommends -in order to ensure legal certainty- that whenever possible, further processing of personal data based on the once-only principle be* ***specified in a legislative instrument****, which provide appropriate safeguards to ensure compliance with data protection law, including the principle of purpose limitation and ensuring data subjects’ rights”*.

Thus, it is clear that consent in the sense of the GDPR is not a requirement for the exchange of evidence, and that the procedural prerequisite of the SDGR of an explicit request should not be conflated with a GDPR consent requirement: **the explicit request obligation may apply even in cases where there is no personal data involved, and inversely a legal basis for the exchange of evidence must exist even when there is an exception to the explicit request requirement. The two obligations – explicit request and legal basis – exist side by side, and are separate.**

In some piloting domains, the choice for a GDPR consent as a legal basis for the exchange of evidence is plausible, but in many (including those where consent is not possible) a different legal basis will need to be relied upon. While the choice can be different from use case to use case, the legal basis will generally be:

* The legal obligation for the competent authorities to transfer evidences under EU or national law;
* The legal obligation for the competent authorities to transfer evidences as a part of the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The choice of an exact legal basis under the GDPR will still require further analysis (as will, of course, other obligations under the GDPR). At present however, it is sufficient to underline that the impossibility of collecting a valid consent from the data subject(s) that would satisfy the requirements of the GDPR – mainly because the consent cannot be freely given as the GDPR requires - is not by definition a blocking point for DE4A use cases.

The main implications of these issues will be examined below.

### Implications of this understanding – implementing an explicit request functionality

#### When and where should the explicit request be made?

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 **priorto using the technical system**. Since user interactions are initiated at the data consumer’s side, it should be the data consuming authority (or a component of the architecture operated by the data consuming Member State) that collects the explicit request. Reliance on the technical system itself to collect the request is arguably already a ‘use’ of the technical system, and reliance on the data providing authority (or that authority’s Member State) would likely be inefficient to implement, since the SDGR requires that the consuming Member State requests the evidence itself after the explicit request from the user is made.

**Thus, the main implementation option is to implement the request at the data consuming Member State’s side,** either by requiring the consuming authority to ask the question (“would you like us to try to obtain this evidence directly from the issuing authority, or do you prefer to provide it yourself?”), or by allocating this task to an intermediary (e.g. the Data Requestor role in DE4A) within the consuming authority’s Member State.

It is worth noting that the same issue as discussed in relation to the preview requirement occurs in this section as well, namely the distinction (if any) between exchange and use. The phrasing of the SDGR refers to the request as a precondition to ‘use’ of the technical system, which is the basis for this deliverable’s position that the request should be collected by the data consuming Member State. If, on the other hand, one would accept the counterposition that the technical system is only ‘used’ when evidence is exchanged, then the explicit request could also be collected through the technical system itself. The discussions on this point between Member States and with the European Commission will be closely followed.

#### What are the exceptions to the explicit request obligation, and how can this be implemented?

In a virtually identical manner as the preview obligation, the SDGR indicates that use of the technical system is only be permitted at the users’ explicit request “unless otherwise provided under Union or national law” (14.4 SDGR). As with the preview exception, experiences in the course of the DE4A project may change our understanding of this principle, but at present there are no known instances (and nor are they likely to exist) of national or EU level laws that explicitly reference the mandatory use of the technical system as such. As a result, the current interpretation of this exception is that likely applies mainly to:

* Evidences which are **publicly available to anyone without any constraints** (e.g. via public websites, open web services, etc.). In such cases, it seems reasonable to argue that automated cross-border exchange without a request is allowed.
* Evidences which are **available to be exchanged between designated competent authorities within the EU** (without constraint to one or several specific Member States). Based on initial discussions, company information that can be exchanged between business registers via the BRIS network seem to be an example, since the BRIS legislation allows competent authorities to exchange information directly in the circumstances covered by that legislation (without the request by the user). In such cases it seems reasonable to argue that automated cross-border exchange without request is allowed via the technical system as well.

It is worth noting that national or European law could also have the inverse impact: rather than just eliminating any need for an explicit request (and permitting exchanges even without users explicitly requesting it), it would also be possible for such laws to oblige usage of the technical system – not only eliminating the requirement of a request, but even invalidating the possibility of choosing alternative means of submission of evidence. In other words, future evolutions in European or national law can significantly impact the scoping of the use of the technical system.

If this understanding proves to be correct, and if DE4A chooses to implement an infrastructure that can also identify and respect the exception to the request obligation, then this also has architectural implications which are again largely identical to those for the preview obligation. Mainly:

* **Competent authorities should be able to query for each Member State a catalogue of types of evidences available to anyone without any constraints, which should be maintained and made available via the technical system.** If an exchange of such evidences is requested, the technical system should be able to detect it via this database and may omit the process of asking for the user’s request. The database can of course be blank if a Member State considers that none of the supported evidences are publicly available to anyone without any constraints.
* **Competent authorities should be able to query for each Member State a catalogue indicating, on a per use-case basis, whether the relevant evidences can be exchanged to specific competent authorities in other Member States.** Again, if an exchange of such evidences in the relevant use case is requested, the technical system should be able to detect it via this database and may omit the request obligation.

Member States could of course also simply choose always to seek the explicit request of the user, eve when this is not strictly legally required, in which case the architectural implications above could be ignored (or at least they could remain un-implemented in DE4A); this presently seems a likely outcome within a number of DE4A piloting activities.

For the avoidance of doubt, it should be noted that the request of the user (where applicable) should be logged, at a minimum by the competent authority that registered it, since it constitutes evidence that this aspect of the SDGR was complied with.

## Data subject rights in the context of the SDG

### Introduction – Data subject rights in the GDPR, and relationship to the SDGR

#### Context – Data subject rights in the GDPR

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[[10]](#footnote-10):

* 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.

In the sections below, we will briefly discuss the principal rights in general (without examining the precise applicability to the SDGR or the technical system). Note that the existence of data subject rights does not necessarily imply that mechanisms to exercise these rights must be built into the technical system itself, as will be examined in the sections below.

It is also worth noting as a preliminary consideration that data subject rights are not always trivial to implement in e-government applications in general, including in SDGR procedures and within the DE4A project. One horizontal recurring challenge is that the user of a procedure may not be the (only) data subject whose personal data would be processed. When e.g. an employee of a company uses the technical system in relation their company, they may also need to provide the personal data of some of their colleagues (e.g. of the administrators of the company). In these cases, data subject rights cannot be granted merely by interacting with the user. By way of example: providing a privacy notice to the user does not result in all other data subjects receiving the required information themselves.

This problem is however not unique to DE4A or the SDGR, and in most situations exceptions are build into data subject rights for situations where data processing activities have an appropriate legal framework and where direct interaction with data subjects is impossible. For instance, the provision of information on data processing of activities is not mandatory when “*(b) the provision of such information proves impossible or would involve a disproportionate effort, […]. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available”*; or when *“(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests*” (Article 14.5 of the GDPR). One or both of these exceptions will often apply in DE4A piloting activities.

##### Transparency and Right of access

Data subjects have the right to obtain from the data controller certain **information** on the nature and scope of data processing activities[[11]](#footnote-11). The type of information that must be made available to them depends on whether data is collected from them or whether the data originates elsewhere, but generally includes the purpose of the processing, the categories of data concerned, the categories of recipient to whom data will be or is being disclosed, the envisaged storage period, or the criteria used to set that period, the existence of the right to request rectification or erasure of personal data or the restriction of the processing or the right to object to the processing or the right to lodge a complaint to the supervisory authority. Furthermore, they are entitled to receive a **confirmation**[[12]](#footnote-12)that their personal data is being processed. They may require a copy of the personal data undergoing processing concerning them.

##### Rights to rectification and to erasure

Data subjects may request and obtain from the controller the **rectification**[[13]](#footnote-13) **of inaccurate data**. However, the necessity of the correction of inaccurate data must take into account the purpose of the processing. In a situation where data is processed for administrative purposes, accuracy is fundamental. Processing inaccurate data could cause harm to the user, e.g. by limiting their rights.

In certain circumstances, data subjects have the right to obtain from the controller the erasure of the data concerning them.[[14]](#footnote-14) There are limitations to this so-called right to be forgotten, e.g. where the processing is necessary for the compliance with a legal obligation.[[15]](#footnote-15) As a result, the right to erasure generally is inapplicable in the governmental context of the SDGR, where data is created, exchanged and further processed in relation to regulated procedures.

##### Right to object

Data subjects have the right to **object**[[16]](#footnote-16) to the processing of their personal data at any time on grounds relating to their situation. As with other rights, this right is limited. It particular, it may only be exercised when the processing is based on the necessary performance of a task carried out in the public interest or in the exercise of a public authority vested in the controller, or when it is based on legitimate interest. Therefore, the right to object is not available when the processing is performed based on a legal obligation[[17]](#footnote-17). Furthermore, to be valid the objection must be based on specific reasons particular to the situation of the data subject. This right to object is not absolute: it can be rejected by the controller if compelling legitimate grounds can be demonstrated for the processing, which override the interests, rights, and freedoms of the individual. The objection to the processing may also be rejected if it is manifestly unfounded or excessive.

In practice, this right to object is likely to be of limited relevance in the context of the SDGR, since exchanges of evidence must, as a general rule, be requested explicitly by the user. If they object to the processing, they can simply refrain from requesting it. Inversely, when it is required Union or national law, according to art. 14(4) of the SDGR, the right to object does not apply under Article 17, 3 (b) of the SDGR.

In cases where the user is not the (only) data subject (e.g. evidence contains information on another person than the user, such as an employee or family member of the user), those other persons could conceivably object to processing, but the data controllers in the context of the SDGR would be able to deny this request on the basis that the processing is required under the SDGR once the request of the user has been lawfully made.

##### Right to restrict the processing

The right to restrict the processing is linked to the data minimisation principle, the accuracy principle, the purpose limitation principle, and the storage limitation principle. The data subject can restrict the processing of their data in the following situations only[[18]](#footnote-18):

1. the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
2. the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
3. the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
4. the data subject has objected to processing.

Therefore the right to restrict processing can only be exercised as a complementary aspect for another principle.

In practical terms, the right to restrict processing of personal data is supported in the SDGR through the prior request and the preview (allowing a check of the accuracy of the data and supporting the lawfulness of the exchange), and through the data minimisation requirement of the SDGR (Article 14.8 stating that “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”). Thus, compliance with the right to restrict processing is to some extent already built into the SGDR.

##### Right to data portability

In certain circumstances, namely when the data is processed based on consent or following a contract, and the processing is carried out by automated means, then data subjects have the right to receive the personal data concerning them that they have provided.[[19]](#footnote-19) In this case, data subjects have the right to receive personal data concerning them, in a commonly used and machine-readable format, and have the right to transmit those data to another controller without hindrance.

This right is largely irrelevant to the SDGR and the technical system, since the right relates to data that the data subjects have provided to the data controller. Evidences under the OOP are however not personal data that the data subject has provided, but rather personal data that a competent authority holds in relation to them. Therefore, even though consent of the data subject is a possible legal basis for the transfer of personal data, this right is unlikely to be used.

##### Right to human intervention

Data subject generally have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her[[20]](#footnote-20). This protects data subjects against fully automated decision making to some extent. However, this right does not apply in a number of cases, including when the processing is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or when the processing is based on the data subject's explicit consent. Given that either or both of these situations will usually apply to the exchanges of evidences, the right will normally not be relevant to the technical system either.

The summary above shows that the availability of individual rights varies depending on the legal basis applied. The table below illustrate the rights available depending on the legal ground used to justify the processing:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Right to withdraw | Right of access | Right to rectification | Right to erasure | Right to restriction of processing | Right to data portability | Right to object |
| Consent | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |  |
| Compliance with a legal obligation |  | ✓ | ✓ | ✓ | ✓ |  |  |
| Task carried out in the public interest |  | ✓ | ✓ | ✓ | ✓ |  | ✓ |

Table 1 : Rights available depending on the legal basis

Therefore, the rights available to the data subjects will vary depending on the legal basis of the processing, and on the administrative procedures requiring the use of the technical system.

### Data controllers and data subject rights in the SDGR

As the summaries above indicate, data subject rights have two global constraints:

* Firstly, they are exercisable **by data subjects**, i.e. the natural persons who are identified or identifiable on the basis of the processing. Users of the technical system are data subjects, but other data subjects can be involved as well (such as the employees and family members of the user, as already mentioned above). This implies that it would be imprudent to assume that the user is the only entity who can exercise data subject rights.
* Secondly, they are exercisable **towards data controllers**, i.e. the organisations that determine the purposes and means of data processing. In the context of the SDGR, the data controllers generally are the competent authorities that are exchanging data, each of whom act as independent data controllers (a controller to controller exchange of personal data). As a result, it is the competent authorities who should support the exercise of data subject rights.

This may appear to be a complicating factor, but from the perspective of the SDGR, the technical system and DE4A, this actually simplifies the matter, since the competent authorities are already required to support these data subject rights as a matter of compliance under the GDPR, and should already have procedures in place to respond to data subject rights requests. The fact that the technical system is used to transfer evidence under the SDGR does not change this outcome.

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.

None the less, **two caveats apply.** Firstly, while the SDGR doesn’t affect existing data subject rights and doesn’t require that the technical system contains functionalities to support data subject rights, it does note in Annex I that **data subjects’ rights should be included as a part of the information to be provided to citizens and business in the Single Digital Gateway**. In simple terms, this implies that the SDG should inform users how they can exercise their rights. This can be done by pointing them to the right contact information, either at an appropriate governance level in a country (national, regional or local), or at a procedural level – this is up the Member States’ discretion, and does not require EU/SDGR level harmonisation. Since it is an information duty only, it is not strictly necessary to develop software modules or functionalities to automatically organise the exercise of data subject rights. This obligation is a part of the Gateway, not of the technical system to be piloted in DE4A.

Secondly, the observations above **assume a fully decentralised model, where no personal data is centrally stored** **by the technical system**. If personal data is stored by the technical system (including metadata such as log files), then centralised information must also be made available to data subjects to allow them to make data subject rights requests in relation to this personal data. Here too, this does not imply that it would be necessary to develop software modules or functionalities to automatically organise the exercise of data subject rights in relation to the centralised components of the technical system.

The rights available depend on the legal basis used. For the implementation of the SDGR several legal bases can be applied for the processing of a personal data through the technical system, either a legal obligation of the controller, or the performance of a task carried out in the public interest or the exercise of an official authority vested in the controller, or consent. Furthermore, the implementation of the SDGR, and the development of the technical system require a piloting phase to test the solution developed. In such circumstances, the consent of the data subjects would be a possible legal base.

In conclusion, within 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. To the extent that the technical system applies a fully decentralised model where no personal data is centrally processed in the technical system, the competent authorities are the sole data controllers, and they can apply their existing data subject rights procedures in SDGR exchanges as well. There is a clear duty to inform the data subjects on the use of the technical system as a part of the processing, but this is an informational duty that has no architectural implications.

### Implementing data subject rights in the context of the SDGR and the technical system

As noted above, it is the responsibility of the data controllers – in principle the competent authorities – to support the exercise of data subject rights. Therefore, the controllers must ensure awareness of the data subjects concerning their rights and provide the means to exercise them.

#### Informing data subjects

One of the main data protection principles is transparency. This means that the data subjects must be informed of the processing of personal data concerning them.

As noted above, this is a duty which is already incumbent on the competent authorities, and which is not affected by the SDGR – other than the fact that the use of the technical system must also be disclosed.

Generally, this information is provided through the privacy policies of the competent authorities. Before piloting, it is worth revisiting these in order to ensure that all relevant information is present and in line with the processing activities of the DE4A project. After full entry into application of the SGDR (and thus after the termination of DE4A), as noted above, transparent notices should also be provided on the Gateway portal site as well. During the DE4A project, it would be useful to provide similar notices on the DE4A website, or preferably to pilot-specific mini-websites. These notices should clearly, succinctly, and simply explain the instances and purposes of the exchange of information in the context of DE4A.

The preview mechanism of the SDGR is an additional opportunity to ensure that the data subjects are informed of their rights, since the preview step already implies active communication with the user. However, it is not mandatory to ‘repurpose’ the preview mechanism to support this function, nor would it be feasible in all cases: the preview obligation has certain exceptions (i.e. one cannot count on the preview to be available as a tool for transparency in all cases), and furthermore the user may not be the only data subject involved (i.e. interaction with the user is not a guarantee that information has been provided to all data subjects). For this reason, complementary and more traditional means of information and exercise of the data subjects’ rights must be retained, such as information notices, contact points etc…

#### The means to exercise the rights

As noted above, there is no specific legal obligation under the SDGR to develop specific tools to support data subject rights in procedures covered by the SDGR. It is legally feasible to rely on existing data subject rights support procedures which already have to be implemented by the competent authorities.

It is clear however that the legal approach taken in the SDGR implicitly supports certain data subject rights, which can be seen by:

* The preview requirement, supporting the right to transparency and access;
* The approval of the exchange after the preview, supporting the right to object to the processing;
* The data minimisation and purpose limitation principles of the SDGR, supporting the right to restrict data processing;
* The prohibition for the technical system to process evidence beyond what is technically necessary for the exchange, and then only for the duration necessary for that purpose, supporting the right to restrict processing.

It would be feasible to build further on this approach and to design a broader personal information management system around the SDGR and the once-only principle – indeed, this possibility was mentioned favourably in the opinion of the European Data Protection Supervisor on the draft SDGR[[21]](#footnote-21), where the Supervisor noted that:

“*transparency and user control should help ensure that individuals are empowered to challenge misuse and prevent the secondary use of data for purposes that do not meet their legitimate expectations.*

*These considerations equally apply to government data sharing in the context where the ‘once-only’ principle is applied. Indeed, in his Opinion 9/2016 of 20 October 2016 on Personal Information Management Systems (PIMS), the EDPS explained that features in information management systems to allow user control can be very useful to enhance transparency and traceability. The Opinion specifically highlighted that public sector bodies can take advantage of these features in order to allow citizens to better manage access and use of their data.*

*Such features could indeed facilitate informing individuals about government data sharing. For example, by looking at their dashboard in their PIMS (and/or by receiving an alert on their smart phones) individuals could keep track of whether their personal data have been transferred between two different public administrations in cases where transfers are defined by law. PIMS can also help individuals to effectively manage their consent for possible further use in cases where their consent is required for such use.*

*Finally, the Opinion suggested that an initiative by public eGovernment services to accept PIMS as a data source instead of direct data collection could add critical mass to the acceptance of PIMS*”.

The European Data Protection Supervisor thus looked favourably on the added value of PIMS, also in the context of the SDGR (and even on the ability of citizens to manage their own data via PIMS and to become acceptable data sources to competent authorities themselves). However, this is a broader policy consideration that was not integrated into the SDGR. Therefore, from a legal perspective, specific means to exercise data subject rights do not need to be integrated into the design or architecture of the technical system, other than by supporting the aforementioned SDGR requirements (preview, approval, data minimisation, and purpose limitation).

## Structured versus unstructured data in the context of the SDGR

### Introduction – Evidence in the SDGR and the concept of structured data

#### Context – evidence in the SDGR

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?

The question is of course highly relevant for DE4A, since it shapes the functionality that must be provided by the technical system. If unstructured evidence falls outside the scope of Article 14 (because it is not considered to be “in an electronic format that allows automated exchange”), this implies that the technical system can be designed using the assumption that any evidence will contain relevant metadata that allows information to be interpreted (including translated where relevant) and automatically processed in the procedures covered by the SDGR.

#### Structured and unstructured data – concepts and degrees of structure

The concept of evidence “in an electronic format that allows automated exchange” can be interpreted and scoped in many ways. A possible ontology for evidences has been circulated within DE4A using the following overview, circulated by the Spanish Ministry of Economic Affairs and Digital Transformation and ATOS:

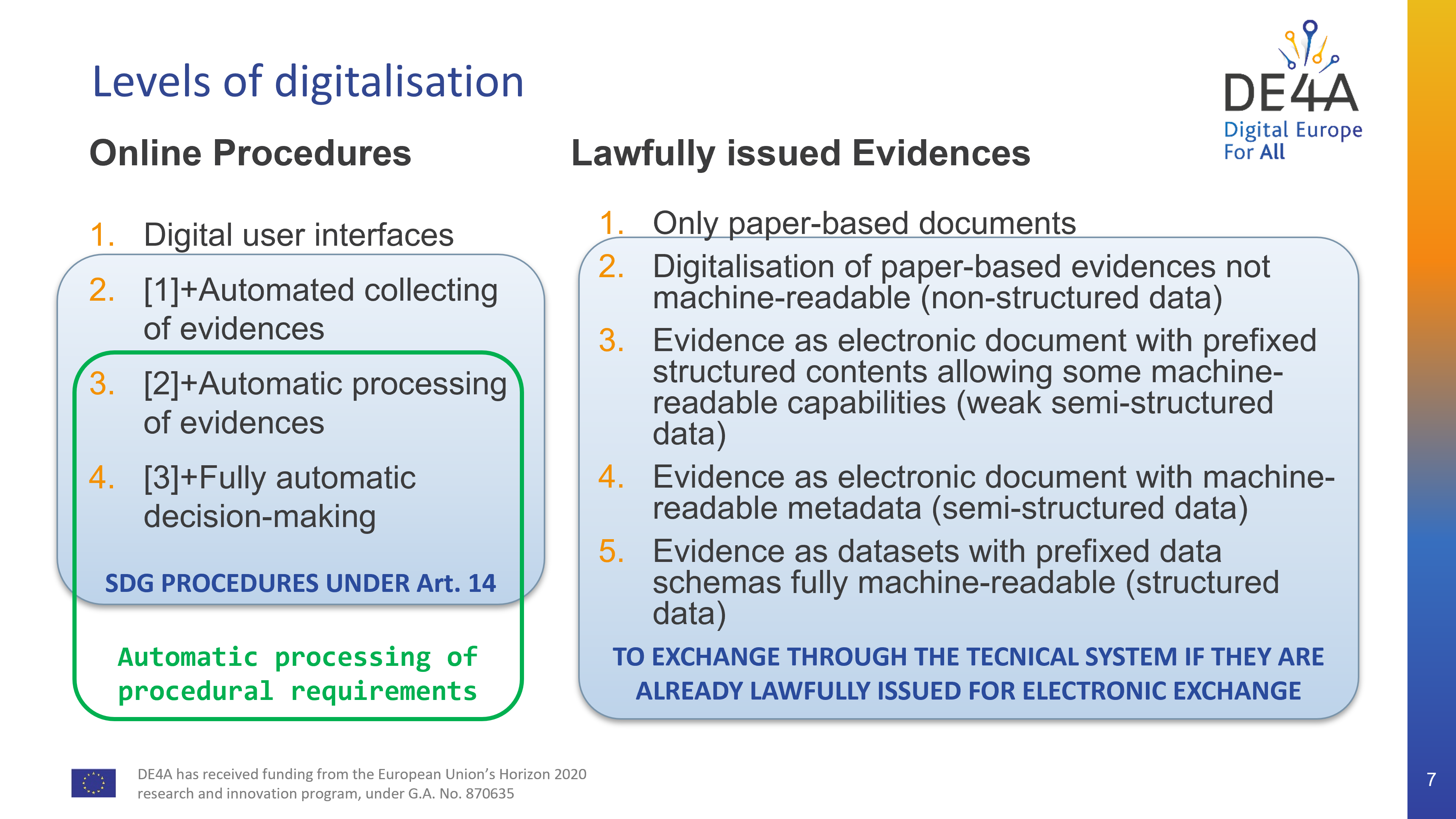


Figure 1: Illustration of fluidity of the concept of "evidence"

The overview illustrates that “evidence” is a fluid concept, that shouldn’t be simply equated to standardised formal documents, comparable to the traditional way of working in an analogue environment (e.g. through standardised birth certificates, statements of domicile, extracts from criminal registers, etc.). In a digital environment, a much more granular approach is possible.

Increasingly, evidences today are no longer supplied as static documents. Rather, evidences are nowadays often available as the result of a dynamic process. For instance, to prove that someone has permission to drive a certain type of car in Austria, it is not necessary to transfer any personal information from data consumer to data provider or vice versa. It suffices to query a register whether a specific person (indicated solely by a cryptographic ID) is allowed to drive. The register only answers „yes“ or „no“, a structured response which is sufficient to automate further reasoning. In this case, the ‘evidence’ is a minimal but perfectly suitable assertion – “yes” or “no”.

The concept of evidences could then be broken up into the following categories:

1. **Only paper-based** documents. These are manifestly outside the scope of Article 14, since they are not issued “in an electronic format”. Member States may have an obligation to digitise the relevant procedures under Article 6 of the SDGR (“Procedures to be offered fully online”), which may in turn result in evidences becoming available in an electronic format; but as long as evidences are only available as paper-based documents, the evidences are legally and functionally irrelevant for Article 14, and also for DE4A.

2. **Digitalisation of paper-based evidences which are not machine-readable**. This category is referenced in this paper as unstructured data – while it is in an electronic format, this is only due to a ‘dumb’ digitisation process that fails to add semantic structure that would allow machine based interpretation of the contents.

3. Evidence as **electronic statements with prefixed structured contents allowing some machine-readable capabilities** (**weak semi-structured** **data**). In this case, the electronic statement has a fixed structure, but lacks metadata (e.g. in the form of standardised XML tags). As a result, the evidence would conceptually allow some machine interpretation, but only provided that the machine in question is programmed to recognise and interpret the structure of the statement even in the absence of metadata (implying that it has either been specifically designed to recognise the specific statement, or that it has strong AI capabilities; neither of which seem particularly viable hypotheses in DE4A or under the SDGR).

4. Evidence as **electronic statement with machine-readable metadata** (**semi-structured** **data**). In this case, the electronic statement has a fixed structure, and also has metadata (e.g. in the form of standardised XML tags), although the metadata scheme is not comprehensive and/or fully standardised. As a result, the evidence allows some machine interpretation (i.e. machine interpretation of some information in the evidence), but not comprehensive – some information will not be automatically interpretable by a machine.

5. Evidence as **datasets with prefixed data schemas fully machine-readable** (**structured data**). In this case, every part of the evidence follows a predefined scheme so that each piece of information in the evidence can be precisely interpreted by a machine, without any need for human interpretation and without ambiguity. As the name suggests, the evidence in this case would be more comparable to a dataset or to an assertion of information, and may not be intuitively recognisable as a ‘document’, i.e. it does not necessarily have a standardised visual appearance that the average citizen would be able to recognise.

6. Evidence as the **result of computational processes**. In this case, computations must be performed dynamically to derive an evidence. These actions may include, but are not limited to, querying registries and interpreting their responses, looking up and interpreting rules, and invoking logical, arithmetic and cryptographic operations on obtained data.

From a functional perspective (and without attaching any legal relevance to this assessment), only categories 5 and 6 allow optimal e-government services, since only datasets that follow prefixed schemas can be certain to contain *only* the precise information that is required for a specific procedure, and to be *fully automatically interpretable* (conceptually including translation where necessary) without human intervention or recourse to e.g. the IMI system for ad hoc cross border support to resolve ambiguities. Furthermore, only category 6 is perfectly suited to ensure proportionality of the evidence, since no other information is provided than what is strictly necessary.

However, this functional perspective does not resolve the legal question examined in this paper: which types of evidence from categories 2-6 above should be considered to be “in an electronic format that allows automated exchange”, and therefore should be supported by Article 14 and the technical system?

#### Provisional note – question to the Commission’s legal service

This particular issue is presently subject to discussions between the Member States. Given that this is a matter of interpretation of a formal European legislative text, a specific question on the issue of structured/unstructured data in the SDGR has been submitted to the European Commission’s legal service. Sent in mid-July, the relevant question was phrased as follows:

*Under article 14.2 of the SDGR, competent authorities that “lawfully issue [relevant evidence] in their own Member State and in* ***an electronic format that allows automated exchange****”, “shall also make such evidence available to requesting competent authorities from other Member States in an electronic format that allows automated exchange”. Should this phrasing be understood as covering* ***any*** *electronic evidences, from the perspective that all electronic evidences (****including unstructured ones****) allow automated exchange, even though unstructured evidences (such as e.g. PDF scans or simple images) would not allow for easy automated processing of the information in the evidences by the receiving competent authority? If so, is there a particular relevance or meaning to the addition “that allows automated exchange” in article 14.2 of the SDGR, since “in an electronic format” already implies exchangeability? Or inversely, should the phrasing be understood as* ***only requiring Member States to exchange information which is structured*** *(i.e. which contains semantic metadata allowing the information to be automatically processed by the receiving competent authority), thus excluding unstructured data? If only structured data must be supported, then would it be compliant with the SDGR to make a distinction on the degree of structure, e.g. distinguishing between electronic evidence with prefixed structured contents allowing some machine-readable capabilities (weak semi-structured data), electronic evidence with machine-readable metadata (semi-structured data), and electronic evidence with prefixed data schemas that are fully machine-readable (fully structured data)?*

A response to this question was integrated into the Commission’s SDG Wiki[[22]](#footnote-22), indicating explicitly that “*Article 14 covers evidence issued “in an electronic format that allows automated exchange”. This includes both structured and unstructured evidence. Furthermore, the OOP WPs are exploring the possibility to also enable a criteria-based approach, that would be similar to the one adopted in the frame of eCertis.”.*

Therefore, the SDGR includes unstructured data within its scope, or at least this is the present working consensus.

### The SDGR and its “electronic format that allows automated exchange”

#### Administrative autonomy and sovereignty of Member States

As the phrasing of Article 14 shows, the SDGR does not contain an obligation for competent authorities (or the Member States) to follow a specific data format (or to apply a specific structure) to electronic evidence that they issue, or even to create electronic evidences that could be used in cross border procedures covered by the SDGR:

“**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)

The phrasing (“*where*” they issue) indicates that the clause is conditional: the authorities must *also* make evidence available in the context of the SDGR *where* it is already issued – if it is not issued in such a format, or if the issued evidence is not relevant to the online procedures, then there is no obligation for a Member State to move to such a format. More simply put: Article 14 does not create a legal obligation to issue electronic evidence at all, let alone to issue evidence in a structured format.

For completeness sake, it is repeated that Article 6 of the SDGR does contain an obligation for Member States to ensure that some procedures are offered fully online, which may result in evidences becoming available in an electronic format if the procedures require evidences; but **the SDGR does not contain a direct legal obligation for Member States to introduce new types of evidences, to provide electronic versions of them, or to apply a specific format or structure to those electronic evidences**.

#### Impacts on the design of the technical system

The more relevant questions are whether requesting Member States in SDGR procedures are required to accept *any* electronic evidence (including those which are entirely unstructured, such as images without relevant metadata) that they receive through the technical system; and whether the technical system must support the exchange of any such unstructured evidences. The questions are of course interlinked: if the technical system would reject evidence that does not incorporate any metadata, then the acceptance of such evidence by requesting Member States is irrelevant, since they would never receive it. On the other hand, even entirely unstructured evidence will be provided in combination with some metadata, since it is provided in response to a request for specific evidence – in other words, contextual information relating to the specific exchange already provides some metadata (e.g. the identification data of the user, the type and format of the evidence, the issuing authority and the issuing date), even if the evidence itself is entirely unstructured.

From a legal perspective, the provisional working assumptions are:

* For the first question, that **requesting competent authorities cannot reject evidence in an unstructured format**. It is the issuing Member State that determines which evidence is lawfully issued and how. There is no legal basis for a receiving Member State (or a receiving competent authority) to reject evidence because it does not meet its formatting/structure expectations. For completeness, it can be noted that a receiving Member State may require additional documentation to be provided, such as translations of the evidence.
* For the second question, that **the technical system must ensure that at least sufficient metadata or some other form of semantic context is included during the exchange, to allow the receiving competent authority to interpret the nature and content of the evidence.** As a result, **the technical system should be designed in a way that allows this metadata or semantic context to be discovered during an evidence exchange,** either because the metadata or semantic context is embedded in the evidence itself (which would be the optimal scenario), or because the exchange is accompanied by metadata that contains the relevant semantic context and corresponding information in the evidence. The use of an evidence assertion as a result of computational processes meets this requirement as well, of course.

The following reasons for this working assumption can be provided. **Firstly**, the SDGR refers to “an electronic format **that allows automated exchange**”. If no metadata would be required, then it would have been sufficient to say “in an electronic format” – without referencing that the format must allow automated exchange. Given the reference to the capability of allowing “automated exchange”, the legislator must have meant to suggest that some further processing should possible beyond pure transmission – otherwise referencing an “electronic format” would have been sufficient.

**Secondly**, the European Commission – DG GROW published the following **question and answer on the SDG Wiki**[[23]](#footnote-23):

“***1. What type of evidence could exchanged using the Article 14 technical system?***

*Article 14 concerns the setting up of a technical system for the cross border exchange of evidence. According to Article 3 (5) of the Regulation, evidence means any document or data, including text or sound, visual or audio-visual recording, irrespective of the medium used, required by a competent authority to prove facts or compliance with procedural requirements (…). While this definition also covers evidence in both paper and electronic format, Article 14.2 limits the type of evidence relevant to the Article 14 once only exchange to evidence (lawfully issued in Member States and) in an electronic format allowing automated exchange.* ***Allowing for automated exchange means that the data in electronic format must be structured in such a way that it allows for machine-to-machine exchange of the data, or automated processing, based on a request from a user, through a competent authority in another Member State****. Evidence issued in paper format only falls outside the scope of the Article 14 exchange.*

*It will be up to the Commission in close cooperation with the Member States to* ***further define in the implementing act referred to in Article 14.9 the exact formats of the evidence that technically fulfil these criteria***” (sic, and emphasis added).

The statement is not entirely conclusive, firstly because it is a FAQ for internal discussion rather than an official interpretation, and more importantly because it interprets the notion ‘structured’ in a different manner than this paper: ‘structured’ in the FAQ appears to imply that enough metadata is available to enable machine to machine *exchange,* which would not necessarily imply enough metadata to allow machine *interpretation* of the data, as this paper argues is necessary. None the less, at least it already supports the notion that some form of structure comprising metadata or other method allowing semantic interpretation is necessary.

**Thirdly,** the **functional requirements that the SDGR imposes on the technical system seem hard or even impossible to respect when no semantic context at all is added to the evidence.** The SDGR requires that the technical system shall:

* allow the processing of the evidence by the requesting competent authority (Article 14.3 (d)), which is significantly more complex for the authority to do when it receives no contextual semantic information;
* ensure an adequate level of interoperability with other relevant systems (Article 14.3 (g)); it is not clear how any degree of interoperability is feasible without semantic structure;
* not process evidence beyond what is technically necessary for the exchange of evidence (Article 14.3 (g)); no such limitation is possible if there is no semantic structure that allows relevant evidence to be extracted;
* 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 (Article 14.8). Again, this limitation is not possible if there is no semantic structure that allows relevant evidence to be extracted.

**Fourthly,** in the absence of semantic information, evidence can only be interpreted through systematic ad hoc human interpretation – in practical terms: unstructured evidence will more often than not require use of the IMI system to verify the authenticity of the provided evidence from the source Member State. This is however not a default path that the SDGR foresees: Article 15 of the SDGR states that “***Where the technical system****, or other systems for the exchange or verification of evidence between Member States are* ***not available or are not applicable****, or where the user does not request the use of the technical system,* ***competent authorities shall cooperate through the Internal Market Information System (IMI)*** *where this is necessary in order to verify the authenticity of evidence that was submitted to one of them in an electronic format by the user for the purpose of an online procedure*”*.*

In other words, IMI is foreseen when the technical system *cannot* be used and automatic exchange or verification is therefore not possible – implying that use of the technical system *should* support automatic exchange and verification, and therefore that evidence exchanged through the technical system should contain semantic information allowing the verification of its contents.

The aforementioned Commission FAQ also seems to take this position, since it contains the following question and answer: “***3. What is the role of IMI?***

*IMI is not a system enabling the exchange of evidence. It enables an authority to get in touch with another EU authority to check conformity of an evidence provided by the user. As foreseen by Article 15 of the SDGR,* ***IMI will be complementary to the once only system, in cases the user chooses not to use once only, or if once only is not available for this specific evidence****.”*

Therefore, the Commission FAQ too sees the IMI system not as a support which can be systematically relied upon when using the technical system, but rather as a complement that is available when once-only under Article 14 is not possible, for whatever reason.

**On the basis of these considerations, it seems reasonable to work on the assumption that evidences under DE4A should contain, or be accompanied by, sufficient metadata or semantic information to allow machine interpretation by the receiving competent authority, that would allow the procedures to be completed without exclusive dependence on human interpretation, including via the IMI system.**

As indicated above, this conclusion is tentative, and subject to evolution depending on the positions taken by the Member States and/or the Commission legal service.

## Charging for evidences under the SDGR

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. It contains a section requiring Member States to ensure that electronic payments are possible for the completion of online procedures, namely Article 13.2 (e), which notes that “*where the completion of a procedure requires a payment, users are able to pay any fees online through widely available cross-border payment services, without discrimination based on the place of establishment of the payment service provider, the place of issue of the payment instrument or the location of the payment account within the Union*”. However, this provision clearly is applicable to the payment by the user of a fee to the competent authority requesting evidences (the data consumer) for the cost of the administrative process. It does not address the payment of a fee to the competent authority providing evidences (the data provider).

It appears that the SDGR is silent on the issue of payment to evidence providers, and therefore 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.

Discussions are currently ongoing between the Member States on the most prudent and effective way to address this topic. Options include an agreement to provide evidences for free for the purposes of SDGR procedures, or to implement a prepayment model where a user can buy a certain amount of credit that could be disbursed between Member States providing evidences. Whether a payment model is adopted and whether that is advisable in light of the complexity of its implementation is however largely a political debate; the legal context of the SDGR provides no particular guidance on this topic.

## Further processing of evidences

The issue of further processing is to some extent inherent to the concept of OOP, and thus also to DE4A. The issue has briefly been addressed in the frame of D10.3 - POPD Requirement n°3 - Further processing but warrants additional reflection.

### Further processing under the GDPR

DE4A supports the implementation of the SDGR and the development of the technical system, as defined in article 14 of the SDGR. Its pilots relate to the exchange of authentic and trustworthy information about citizens and businesses, originating directly from official registers. Pilots are organized across three different pilot streams: Studying Abroad, Doing Business Abroad, and Moving Abroad. In each stream, multiple use cases will be piloted, based on existing laws and administrative procedures.

The OOP, and DE4A’s pilots, therefore, rely essentially on the reuse of data previously created, collected or stored by public administrations in relation to citizens and businesses; indeed, such reuse is even its sole purpose. Where the information exchanged through the application of the OOP includes personal data, issues concerning ‘*further processing’* as described under the GDPR must be addressed. The notion of further processing, which is processing of personal data beyond the initial purpose for which it was collected, is tied to the notion of purpose limitation.

Under the GDPR, purpose limitation is a fundamental data protection principle according to which data is collected for specified, explicit and legitimate purposes and may not be further processed in a manner that is incompatible with those purposes (Article 5.1 GDPR). There are exceptions, when the data subjects consented to the further processing or when or when it constitutes a necessary and proportionate measure in a democratic society to safeguards certain of its fundamental elements (such as listed in article 23 of the GDPR). As highlighted by the European Data Protection Supervisor, easing administrative burdens on individuals or organisations is one of the primary aims of the OOP, and is undoubtedly of public interest 58. None the less, processing of personal data for other purposes should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected (Recital (25) GDPR).

The compatibility of purposes must be assessed based on the link between the new purposes, the context of the processing, the nature of the data concerned, the possible consequences of the processing and the existence of appropriate safeguards (Article 6.4 GDPR). In the case of further processing through the technical system set up in compliance with the SDGR, the compatibility of purposes is largely governed by the legislator at EU level: the existence of the SDGR and its explicit requirement to apply the OOP in the enumerated procedures, under the safeguards stated in the SDGR, fundamentally implies that the further processing required by the SDGR is considered as compatible with the original purposes by the legislator. Of course, DE4A’s compliance with the safeguards of the SDGR is critical in this assessment, and notably the obligation in principle to only use the technical system at the explicit request of the user, or when required under Union or national legislation.

On this basis, the further processing of personal data under DE4A must *prima facie* be deemed as compatible with the original purposes. Under data protection law (GDPR and EUI-GDPR), if the purposes of processing are not incompatible, no new legal bases need to be applied.

Even disregarding this point, when transferring evidences through the technical system, further legal bases for the transfer can be identified. Specifically:

* For some pilots, the only personal data being transferred will be relate to the user himself. In those cases, the **consent** of the user is a viable legal basis. Of course, this implies that the consent must be freely given, specific, informed, and unambiguous. These requirements cannot be satisfied in all cases. Notably, when a user is required to provide evidence in order to satisfy their legal obligations, it is questionable whether the consent is freely given. For that reason, consent is not a reliable legal basis for all piloting activities.
* In the cases of administrative procedures, there are two further legal bases that can be applied, either the **performance of a legal obligation**, or the **performance of task of public interest or the exercise of official authority vested in the controller** (the latter being the piloting public administration) (Article 6.1. (c) and (e)). In hypotheses where there is no national legislation organising the procedure, but when the procedure falls under the mandate of the competent authority concerned by the transferred, the legal bases will typically be the performance of task of public interest or the exercise of official authority vested in the controller.

The exact choice of a legal basis will vary between the three pilot streams (Studying Abroad, Doing Business Abroad, and Moving Abroad), or even between the use cases piloted in each stream. The DE4A consortium will ensure that at least one of the aforementioned legal bases will always be applied for further processing in DE4A. This, in combination with the compatibility check mentioned above, is sufficient to ensure the legal basis of further processing in DE4A from a GDPR perspective.

### Further processing under the SDGR

The section above examines only the legal challenges related to further processing under the GDPR. However, a broader question is whether, once a data consuming authority has received the evidence in accordance with the SDGR, they can share it with additional authorities within their own country.

While this issue is still open to discussions, it is clear that the SDGR governs 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.

By way of example: if a user uses the technical system to move to a new country, the SDGR will e.g. help them by transferring all relevant evidences, which may cause them to get registered in a civil register (if that exists in a Member State). Being in a register will likely trigger many follow-up actions and transfers of the data, which may include the evidences that were transferred: the civil register may e.g. notify the competent tax authorities that there’s a new resident who needs to pay residence taxes, or the evidences may need to be kept in an official archive under national archiving laws. While transfers of evidence are likely not the default situation, they may still occur in some cases (such as archiving obligations), under national legal frameworks. All of these uses however are subject only to national laws, which are not affected by the SDGR. As recital (26) to the SDGR notes, “*This Regulation should also not affect the procedural workflows within and between the competent authorities, the ‘back office’, whether digitalised or not*”.

For the avoidance of doubt, it is clear that the SDGR also contains a purpose limitation principle, which notes explicitly 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*” (Article 14.8). However, it would appear logical that use of the evidence “for the purpose of the procedure” must include any use that’s mandatory under national law as a result of that procedure. Otherwise, use of the SDGR would make it impossible for receiving competent authorities to respect national laws, such as archiving laws, or e.g. communication with the citizen on topics like community taxes, garbage collection, road repairs, or anything else that would naturally and legally follow from the completion of an administrative procedure. This processing falls outside of the scope of the SDGR and is entirely governed by national law. Otherwise, all Member States would have to create exceptions in their national laws that allow this data to be reused whenever their laws require it, *except* if it reached their competent authorities under the SDGR, which would not be workable.

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

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, as also discussed in section 3.2 above. However, the concern is not limited to evidence containing personal data, since even competent administrations that process solely non-personal data (e.g. company data which does not contain references to individual persons) will be bound by their legal remit in making such data available, which may not permit exchanges to authorities in other countries.

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 should choose to explore exchange patterns that fall outside of the limitations of the SDGR, a separate legal basis would be needed, separate from the SDGR. This is one of the principal reasons why some Member States strongly favour an USI pattern, since this allows data providing competent authorities to communicate evidences directly towards the relevant citizens and administrations. Insofar as this has a clear legal basis under their national laws – which appears to be broadly the case, based on the Member States’ own assessments – this could resolve the issue of a legal basis.

To mitigate these issues to some extent, Member States are discussing whether it would be necessary or beneficial to further scope their piloting activities, e.g. through a Memorandum of Understanding, as was also done in prior Large Scale Pilot projects. This issue will be monitored and supported further by WP7.

# Preliminary ethics assessment

## Provisional note on the scoping and impact of ethics under DE4A

DE4A project’s ethics requirements are managed in detail within Work package 10 - Ethics Requirements. In the sections below, we will summarise the resulting actions which have already been undertaken. 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

With respect to ethics, the principal challenges relate to compliance with data protection safeguards and the requirements of the SDGR. The DE4A project adheres to the EU’s framework for Responsible Research and Innovation (RRI)[[24]](#footnote-24). As described by the Commission, RRI implies that societal actors (researchers, citizens, policy makers, business, third sector organisations, etc.) work together during the whole research and innovation process in order to better align both the process and its outcomes with the values, needs and expectations of society.

The objective of the ethics tasks in DE4A is to ensure that the innovation brought about by the project is in line with European ethics and moral values, including:

- 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

In practical terms, however, a key consideration is that the DE4A project builds on the policy background of the adopted SDGR. As such, DE4A is an e-government project which aims to facilitate the electronic exchange of information in administrative proceedings where this information thus far is usually done on paper. As such, 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. It does so within a confined, regulated space, namely within the rules of the SDGR.

This also limits the scoping of ethics assessment within the project, since DE4A’s remit is not to assess the ethics behind the choices made by the legislator in the SDGR, nor the ethics behind the underlying administrative procedures that are supported by the technical system under the SDGR. In other words, DE4A must reasonably assume that the SDGR and these administrative procedures are ethical in and of themselves, and limit itself to the implementation choices that the project itself makes.

## Measures taken

The consortium, in compliance with its ethics obligations, has appointed a DPO, drafted guidelines and template to inform and collect consent of pilot users, and analysed the risks linked to further processing, through the deliverables referenced above. In the sections below, we will summarily describe these actions.

### Appointment of a DPO

The DE4A consortium appointed a Data Protection Officer[[25]](#footnote-25) 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 persona 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 member who are public authorities are required, under article 37.1 (a) of the GDPR to appoint a data protection officer. The DE4A DPO cooperates with and supports them, to provide data subjects with information and support in their own language.

The contact details of the DPO have been added to the privacy policy of the website and will be included in information provided by the DE4A consortium related to the processing of personal data, including in future piloting effects, to support the requirements of transparency and justice.

### Information and consent scheme

Under the GDPR, any data controller, which is the entity, who alone and jointly with other 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 have been implemented for the purposes of DE4A.

* A 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, the ethics work considers that in many cases piloting will be done on the basis of the consent of the users. To be valid under the GDPR consent must be freely given, specific, informed and unambiguous. Therefore, adequate information on the processing must be provided to the user/ data subjects. D10.1 provides guidelines and templates for the consortium member to inform data subject and obtain their consent, following the requirement of article 13 of the GDPR. These include:
  + the identity and the contact details of the controller and;
  + the contact details of the data protection officer;
  + the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
  + where the processing is based on them, the legitimate interests pursued by the controller or by a third party;
  + the recipients or categories of recipients of the personal data, if any;
  + where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation.
  + the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
  + the existence and means to exercise data subjects rights;
  + the right to lodge a complaint with a supervisory authority;
  + whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
  + the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

Deliverable D10.1 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 is provisional, given that pilots are still undergoing revisions and scoping; the templates will be maintained and adapted as the project progresses.

### 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 section 3.6 above.

Overall, because further processing is likely to arise during the pilot phase of DE4A, specific measures are implemented to minimize the risks to the rights and freedoms of the data subjects:

* Further processing only occurs at the explicit request of the user. Therefore, the user will have the possibility to preview the relevant information as required by the SDGR, and to prevent the further processing if they feel that the preview causes concerns.
* Pilot user will be adequately informed using the standardised information documents provided in D10.1 – POPD Requirement n°1 – Identification and recruitment of participants;
* The DPO contact information will be readily available to the pilot’s users, should they need additional information, and wish to exercise their data subjects’ rights (see D10.2: POPD - Requirement No. 2 – Data Protection Officer)
* The DPO will support the beneficiaries by responding to data subject rights requests appropriately, and will facilitate interactions between the competent authorities involved in any specific exchange;
* Stringent security controls will be systematically implemented e.g. authentication of data sources, authentication of data recipients, systematic logging, data minimisation controls, preview and verification procedures, and encryption of data in transfer.

# Data flow assessment and national or pilot specific requirements

## Relevance of the preliminary data flow assessment

A data flow assessment is a preliminary step to the preparation of a data protection plan and a data protection impact assessment (as described in the GDPR). This preliminary assessment allows the identification of the main elements of a planned or tentative processing activity. Specifically, it should:

* Identify the categories of data processed and purposes (i.e. purpose limitation): is necessary to identify the object of the processing activity. This is necessary to be able to adequately inform data subjects (i.e. transparency of processing activity), determine what is needed specifically for the processing (i.e. data minimisation principle). The information gathered here will points towards the most adequate legal base for the processing.
* Identify the basis of the processing: this is a key element; without an adequate legal base the processing is illicit (i.e. lawfulness principle). The legal base not only influences the validity of the processing but also the rights of the data subjects (and thus the obligation of the controllers). This also bears heavily on the possibility of further processing
* Identify the data transfers, i.e. movement of data and data recipients. The movement of data, the recipients and storage of data are the fundamental elements of the processing. Recipients also covers recipients withing an entity. Those elements must be included in the information provided to the data subjects, but they also are important for the determination the appropriate safeguards that should be implemented (i.e. integrity and confidentiality principle).
* Identify actors (i.e. controller, processors, data subjects). This supposes to know what the attribution of each actors are, which one is in charge and determine the means and purposes of the processing, and which ones acts one behalf of the other, and on its instruction. Identify the actors of a processing authority is fundamental to attributes responsibility for the processing, vis-à-vis the data subjects but also vis -à-vis the other actors. Based on a clear attribution of responsibilities adequate contractual documents can be drafted to frame and organize the processing.
* Identify the safeguards in place and to implement based on the identified flow and data and actors involved, the risks can be assessed, and adequate safeguards identified.

In the sections below, we will summarise DE4A’s general model for data exchanges, as well as current working assumptions in relation to responsibilities.

## General DE4A approach and working assumptions in relation to responsibilities

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 discuss several possible patterns to implement the OOP, most of which are likely to 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, and as falling within the scope of the SDGR.
* The typical legal basis is ‘processing is necessary 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 as explained in section 3.2 above, 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 2: Primary intermediation pattern, see D2.1

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.

Based on the current conceptual model, from a data protection perspective, all data providers and data consumers (i.e. all competent authorities as defined under the SDGR) are considered to be separate and independent data controllers, each of whom are solely responsible for their own processing activities, and without assuming joint responsibility towards the data subject for data processing occurring within the context of the SDGR. This is justified by the fact that they do not share any common purpose; all participants act only to fulfil their own legal remit. The exchange of evidence (to the extent that it contains personal data) is thus considered to be a transfer of personal data from controller to controller.

The administration of the technical system is ultimately (i.e. after the entry into application of the SDGR and beyond the context of DE4a) to be performed by the European Commission. It is possible that this centralised infrastructure will process personal data as well, notably if it plays a role in communicating the explicit requests, or as a gateway for eDelivery of the evidence exchanges. If so, then the operator of the technical system – the European Commission – would likely be qualified as the data controller for such centralised personal data processing.

The user will in principle be a data subject as defined in the GDPR, but given some of the administrative procedures foreseen in the SDGR, other data subjects than the user can also be involved in an exchange, e.g. when a parent authorises an exchange relating to their household, or when an administrative employee authorises transfers relating to colleagues. In such cases, representative mandates or powers need to be proven; otherwise, such users cannot be involved in the procedure.

## National or pilot scenarios specificities

Each piloting stream may face additional legal challenges when developing their use cases. Without going into detail at the present stage, this section provides an initial overview of piloting plans and potential legal challenges. These will be elaborated further as DE4A evolves.

### 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.

|  |  |  |
| --- | --- | --- |
| **SDGR Procedure** | **DE4A Studying Abroad pilot use case** | **Categories of data used** |
| 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 | Personal identification data,  Government issued identification data  Information concerning higher education  Information concerning family members  Financial identification data  Financial resources  Financial assistance |
| Submitting an initial application for admission to public tertiary education institution | Use case 1: Application to public higher education | Personal identification data,  Government issued identification data  Information concerning higher education |
| Requesting academic recognition of diplomas, certificates or other proof of studies or courses | Use case 3: Diploma recognition | Personal identification data,  Government issued identification data  Information concerning higher education |

Table 2 : Categories of personal data used in the Studying abroad pilot

### 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.

### Moving Abroad

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

|  |  |  |
| --- | --- | --- |
| **SDGR Procedure** | **DE4A Moving Abroad pilot use case** | **Categories of data used** |
| Registering change of address | Registering a change of address | Personal identification data |
| Citizens’ and family rights | Requesting civil status certificates | Personal identification data  Information on civil status |
| Requesting information on the data related to pension from compulsory schemes | Requesting information on the data related to Career overview, pension simulation and claiming pension and pre-retirement benefits | Personal identification data  Personal particularities  Particularities regarding pension  Professional employment |

Table 3: Categories of personal data processed in the Moving Abroad pilot

The principal challenge, beyond the inherent sensitivity of some of the data, is in ensuring lawfulness of the exchange. To the extent that the procedures are scoped in a manner that ensures that only the user themselves are affected (in simpler terms: that a citizen can change their own address, but not the address of other members of their household), in this particular use case consent is likely a viable legal basis to justify data processing under the GDPR.

# Conclusions

As the preceding sections will have shown, there are many uncertainties still on the exact interpretation of the SDGR. These will be reduced in future work, both as a result of project internal discussions, and driven by feedback from Member State discussions and from the European Commission in the further elaboration of the SDGR.

None the less, a few key conclusions and findings can already be forwarded at this stage on the legal framework and the requirements that it imposes on the technical system. These can be summarised succinctly as follows:

|  |  |
| --- | --- |
| Legal requirements for the technical system | |
| Preview of evidence | |
| 1.1 | The system must be capable of offering a preview possibility to the user before the consuming authority is permitted to use it. |
| 1.2 | As a working assumption, the system should organise the preview of evidence with the data providing Member State (either the Data Owner or the Data Transferor), or with the data consuming Member State through the Data Requestor, or with the user. At any rate, evidence should be shielded from use by the Data Evaluator until the evidence exchange is approved. |
| 1.3 | The system must include a verifiable (logged) functionality that ensures that evidence is not retained within the technical system after the user decides whether or not to proceed with the exchange. |
| Explicit request | |
| 2.1 | As a working assumption, the system should implement the request functionality at the data consuming Member State’s side |
| 2.2 | The request requirement is not equivalent to a consent as defined in the GDPR. To the extent that data protection law applies to an individual exchange, a legal basis should be found on a case by case basis. The legal basis may be consent, but this is not the default situation. |
| Data subject rights | |
| 3.1 | The SDG must provide information to the user on how to exercise their rights, as must the relevant competent authorities. |
| 3.2 | However, no part of the SDGR requires technical components to be built into the technical system that enable or support the exercise of data subject rights |
| Structured and unstructured data | |
| 4.1 | Requesting competent authorities cannot reject evidence in an unstructured format. It is the issuing Member State that determines which evidence is lawfully issued and how. |
| 4.2 | The technical system must ensure that at least sufficient metadata or some other form of semantic context is included during the exchange, to allow the receiving competent authority to interpret the nature and content of the evidence. |
| Charging for evidences | |
| 5.1 | The SDGR does not affect an evidence issuing authority’s ability to charge for evidences, including for procedures under the SDGR that exchange evidences through the technical system. |
| Further processing of evidences | |
| 6.1 | Exchanges of evidences under the SDGR will nearly always constitute further processing as defined under the GDPR; however, this is not problematic since the SDGR creates a clear legal basis and legal safeguards for the further processing. |
| 6.2 | As a working assumption, the SDGR is not considered to have an impact on further processing of evidences that take place *after* the exchange via the technical system. These are governed purely by national law. |
| Lawfulness / legal basis of piloting prior to the comprehensive entry into application of the SDGR | |
| 7.1 | As a working assumption, at least for data protection purposes, piloting activities falling within the scope of the SDGR use cases have a lawful legal basis on the grounds that the SDGR has been adopted and will become effective at the end of 2023, and that piloting can therefore 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. Member States that do not accept this reasoning can choose to pilot using fake or fictitious data, or seek an alternative legal basis for processing personal data, e.g. based on the consent of the data subject for fictitious procedures. |

Table 4: Legal conclusions on system requirements

Furthermore, some points of discussion and elements of differences and similarities between the Member States can also be highlighted at this point. These can be particularly useful as a way to assess potential legal red flags in piloting activities:

|  |  |
| --- | --- |
| Differences and similarities between the Member States | |
| Legal basis and interaction patterns | |
| 1.1 | All Member States **agree** on the strong supporting role of the SDGR in providing a legal basis for the development of a technical system.  Similarly, all Member States **agree** that national laws can create a legal basis for data providers to directly issue evidences to a requesting user in an USI pattern. |
| 1.2 | There is however **no consensus** between the Member States as to whether the SDGR is a sufficient legal basis for piloting in DE4A prior to its comprehensive entry into force in 2023.  Furthermore, there is **no consensus** on whether the USI could satisfy the requirements of the SDGR, or whether it complies with the OOP in general.  Finally, there is **no consensus** on whether the SDGR comprehensively overrides any national requirements in relation to once-only exchanges (e.g. whether national requirements could be imposed on foreign competent bodies prior to permitting an exchange). |
| Data subject rights | |
| 2.1 | All Member States **agree** that the use of the technical system as such does not impose additional requirements in relation to data subject rights. |
| Structured and unstructured data - proportionality | |
| 3.1 | All Member States **agree** that unstructured data is also eligible to be exchanged as evidence under the SDGR, and that such domestic evidence (including unstructured evidence) may be accompanied by structured canonical evidence that would assist in the interpretation of the domestic evidence. |
| Charging for evidences | |
| 4.1 | There is **no consensus** between the Member States as to whether the SDGR provides a legal basis or contains any legal requirement to support a payment functionality for evidence issuing. |
| Further processing of evidences | |
| 5.1 | All Member States **agree** that the use of exchanged evidences in procedures under the SDGR is lawful, even if it would constitute further processing. |
| 5.2 | There is **no consensus** between the Member States as to whether the SDGR prohibits receiving competent authorities to further process (or exchange) received evidences if this would be required under national law (i.e. whether the SDGR interferes with such national legal frameworks). |

Table 5: Similarities and differences between the Member States

It is intended that the findings of this report and its working assumptions will be further refined and adjusted, based on future discussions and working experiences in DE4A.

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

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> [↑](#footnote-ref-1)
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> [↑](#footnote-ref-2)
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> [↑](#footnote-ref-3)
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>. [↑](#footnote-ref-4)
5. See also the EDPS Opinion 8/2017 on the proposal for a Regulation establishing a single digital gateway and the ‘once-only’ principle; available at <https://edps.europa.eu/sites/edp/files/publication/17-08-01_sdg_opinion_en_0.pdf> [↑](#footnote-ref-5)
6. Requiring that: “Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed” [↑](#footnote-ref-6)
7. Available at <https://ec.europa.eu/cefdigital/wiki/display/SDGOO/Legal+-+SDG+OOP> [↑](#footnote-ref-7)
8. ‘Imbalance of power’ in consent is addressed by the European Data Protection Board in the Guidelines 05/2020 on consent under the Regulation 2016/679, adopted on 4 May 2020, p. 9, <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [↑](#footnote-ref-8)
9. See <https://edps.europa.eu/sites/edp/files/publication/17-08-01_sdg_opinion_en.pdf> [↑](#footnote-ref-9)
10. See <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/what-are-my-rights_en> [↑](#footnote-ref-10)
11. See the Guidelines on Transparency under Regulation 2016/679 from the Article 29 Working Party, <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025> [↑](#footnote-ref-11)
12. Article 15 GDPR. [↑](#footnote-ref-12)
13. Article 16 GDPR. [↑](#footnote-ref-13)
14. Article 17 GDPR. [↑](#footnote-ref-14)
15. Article 17.3(b) GDPR. [↑](#footnote-ref-15)
16. Article 21 GDPR. [↑](#footnote-ref-16)
17. However, when the processing is performed based on consent, data subject may withdraw their consent, effectively objecting to the processing henceforth. [↑](#footnote-ref-17)
18. Article 18 GDPR. [↑](#footnote-ref-18)
19. Article 20 GDPR. [↑](#footnote-ref-19)
20. Article 22 GDPR. [↑](#footnote-ref-20)
21. See <https://edps.europa.eu/sites/edp/files/publication/17-08-01_sdg_opinion_en_0.pdf> [↑](#footnote-ref-21)
22. Available at <https://ec.europa.eu/cefdigital/wiki/display/SDGOO/FAQ> [↑](#footnote-ref-22)
23. Available at <https://ec.europa.eu/cefdigital/wiki/display/SDGOO/FAQ> [↑](#footnote-ref-23)
24. See <https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation> [↑](#footnote-ref-24)
25. See D10.2 POPD Requirement n°2 [↑](#footnote-ref-25)