

D10.5 GEN Requirement n°5 – Periodic report by the Ethics Advisor

|  |  |  |  |
| --- | --- | --- | --- |
| Document Identification | | | |
| Status | Final | Due Date | 31/12/2020 |
| Version | 1.0 | Submission Date | 18/12/2020 |

|  |  |  |  |
| --- | --- | --- | --- |
| Related WP | WP10 | Document Reference | D10.5 |
| Related Deliverable(s) | WP4, WP7, WP8, WP9 | Dissemination Level (\*) | CO |
| Lead Participant | TLX | Lead Author | Ruben Roex (TLX) |
| Contributors | TLX | Reviewers | Name (PartnerName); |
| Name (PartnerName); |

|  |
| --- |
| **Keywords :** |
| Ethics, management, piloting, data protection |

Document Information

|  |  |
| --- | --- |
| List of Contributors | |
| Name | Partner |
| Ruben Roex | Timelex |

|  |  |  |  |
| --- | --- | --- | --- |
| Document History | | | |
| Version | Date | Change editors | Changes |
| 0.8 | 15/12/2020 | Ruben Roex | Initial version of document |
| 0.9 | 16/12/2020 | Julia Wells | Quality check for submission |
| 1.0 | 17/12/2020 | Ana Piñuela | Final for submission |

|  |  |  |
| --- | --- | --- |
| Quality Control | | |
| Role | Who (Partner short name) | Approval Date |
| Deliverable leader | Ruben Roex (TLX) | 15/12/2020 |
| Quality manager | Julia Wells (ATOS) | 16/12/2020 |
| Project Coordinator | Ana Piñuela Marcos (ATOS) | 17/12/2020 |

Table of Contents

[18/12/2020 1](#_Toc59118117)

[Document Information 2](#_Toc59118118)

[Table of Contents 3](#_Toc59118119)

[List of Acronyms 4](#_Toc59118120)

[Executive Summary 6](#_Toc59118121)

[1 Introduction 7](#_Toc59118122)

[1.1 Purpose of the document 7](#_Toc59118123)

[1.2 Structure of the document 7](#_Toc59118124)

[2 Methodology of the ethics assessment 8](#_Toc59118125)

[2.1 Responsible Research and Innovation and Value Sensitive Design 8](#_Toc59118126)

[2.2 DE4A’s normative framework and ethics requirements 8](#_Toc59118127)

[3 Object of evaluation: the OOP in European law and policy 10](#_Toc59118128)

[3.1 General functional description of the once-only principle 10](#_Toc59118129)

[3.2 Ethical implications – priorities for ethics evaluation 10](#_Toc59118130)

[4 Object of evaluation - DE4A’s approach to the once-only principle and the SDGR 16](#_Toc59118137)

[5 Conclusions 17](#_Toc59118138)

[References 18](#_Toc59118139)

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 |
| 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 Principle, <http://www.toop.eu/> |
| TOOP | The Once Only Project |
| ZKP | Zero Knowledge Proof |

Executive Summary

The Periodic Ethics Report assesses compliance of the DE4A project with ethical requirements, taking into account European values and principles, in particular for EU funded research projects. This is the first iteration of the Ethics Report, describing ethical challenges that the project faces, and relevant decisions taken within the first 12 months of the project.

The report is based on the EU’s framework for Responsible Research and Innovation (RRI). 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.

Within this report, the ethics assessment focuses on the ambitions, realisations and foreseeable impacts of the DE4A project, and more generally of the once-only principle as envisaged under EU policies regarding the Single Digital Gateway. This first report focuses only on the first year of the project, including scoping, architectural design, planning and research. Impacts in practice cannot be observed or assessed yet, as piloting has not yet been initiated. This report therefore assesses ethical compliance of current planning, and posits ethical requirements for the continuation of the project. Compliance with these requirements will be evaluated in the future Ethics Reports.

Briefly summarised, based on the current ethics assessment, the DE4A project is largely in line with the EU’s ethical requirements. Two ethical challenges are identified which should be monitored and evaluated as priorities in the reminder of the project:

* **Data protection**. The EU has a high bar for the protection of the fundamental right to protection of personal data, as enshrined in the Charter of Fundamental Rights and in the General Data Protection Regulation (GDPR), among other points. In order to respect the EU’s values of data protection (comprising also aspects of privacy protection), a data protection impact assessment (DPIA) should be conducted to ensure that the personal data of European citizens is respected. While the European legal framework in relation to once-only exchanges provides a critical set of data protection constraints, it is not certain at this stage whether all DE4A piloting activities will remain strictly within the confines of that legislation. In particular when exploring innovative implementations of the once-only principle, a DPIA would be strongly recommended to mitigate data protection challenges.
* **Equality and citizen’s rights, including the right to good administration**. The once-only principle, as envisaged in European law and in DE4A, relies on the voluntary participation of citizens and/or business. While this protects them against exchanges which are invisible or not transparent to them, it also implies that the benefits of the once-only principle are only available to digitally literate persons who are capable of requesting it, and that the individual interest takes precedence over societal interests. This is a valid policy choice, but it is recommended to explore what the implications are, and to evaluate whether this policy choice is ethically optimal.

These priorities should continue to be promoted within the project, and future reports will re-evaluate whether the project is fully in line with these requirements.

# Introduction

## Purpose of the document

This first Periodic Ethics Report has been drafted with the objective of assessing compliance of the DE4A project with ethical requirements within the first 12 months of the DE4A project, and defining specific points of attention. Given the timing, this assessment focuses on the ambitions, realisations and foreseeable impacts of the DE4A project as such.

The scoping of the project was taken as a baseline, based on the currently available architectural information and on the functional description of the pilots, as described in the project proposal (the Description of Work[1]) and notably the following deliverables:

* D1.1 Member state eGovernment Baseline
* D1.7 Legal, technical, cultural and managerial barriers
* D2.1 Architecture Framework
* D2.4 Project Start Architecture (PSA), first iteration
* D4.1, D4.5 and 4.9, containing use cases definition and requirements for the three piloting areas
* D7.1 Overview of legal and ethical requirements

While this assessment does not aim to evaluate the ethics behind existing EU or national policy and legislation outside of DE4A, it would not be feasible to assess ethics without considering the policy and legal choices made concerning the interpretation and scoping of the once-only concept. For that reason, this assessment report also considers the ethical implications of the once-only approach adopted by the Single Digital Gateway Regulation, and the exploration thereof in DE4A.

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. This report does not assess the ethics behind these use cases as such – it assumes that existing Member State and EU laws and policies relating to cross border mobility are ethical, or at least that the ethics behind these laws and policies do not require assessment within DE4A.

The report therefore takes as a baseline that existing EU and national laws and policies related to the use cases are ethically sound, and that this report should not evaluate or criticise these. The question assessed in this report is whether the choices that will be made by the DE4A project are ethically justifiable and in line with the EU’s moral values.

## Structure of the document

This document is divided into four main sections:

* Section 2 explains the basic methodology of this assessment, notably the use of Value Sensitive Design techniques and the moral values to be assessed in particular;
* Section 3 describes the object of the assessment, namely the once-only principle at the conceptual and architectural level;
* Section 4 briefly describes the choices made by DE4A in particular.
* Conclusions and focus points for attention are then presented in Section 5.

# Methodology of the ethics assessment

## Responsible Research and Innovation and Value Sensitive Design

Methodologically, the report is based on the EU’s framework for Responsible Research and Innovation (RRI)[2]. 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 the DE4A project is to ensure that the innovation brought about by the project is in line with European ethics and moral values. This is done by applying the theory of Value Sensitive Design[3], an approach which aims to integrate a wide range of human and moral values into the design of (information) technology.

In other words, Value Sensitive Design implies that a normative framework is defined, and that the designers of a system – in this case the DE4A consortium – integrate this framework into their work, thus recognising that systems are rarely ethically neutral, and that human well-being, human dignity, justice, welfare, and human rights can be served by integrating them into technological design.

Therefore, as a first step, a usable normative framework must be established for the DE4A project, and specific ethics requirement must be derived on the basis of this framework. Thereafter, we can assess to what extent the DE4A project already complies, and which requirements warrant particular attention in the future.

## DE4A’s normative framework and ethics requirements

Any ethics evaluation requires an explication of the normative framework against which the anticipated innovation is to be assessed. The DE4A Description of the Action already makes it clear that the central ethical concern is compliance with the fundamental right to data protection. More broadly however, this report assesses the extent to which the project complies with European values as enshrined in the Charter of Fundamental Rights of the European Union – which includes, but is not limited to, the right to data protection and privacy.

With respect to **data protection and privacy**, the OOP must be implemented in a way that safeguards these fundamental rights for natural persons. As stated in the General Data Protection Regulation (GDPR), this implies compliance with the principles of:

o **lawfulness, fairness and transparency**;

o **purpose limitation**;

o **data minimisation**;

o **accuracy**;

o **storage limitation**;

o **integrity and confidentiality**;

o **accountability**.

However, the remit of ethics and the scope of European values is broader than data protection and privacy alone. The Charter applies a structure of six value domains, each of which warrant specific scrutiny in this project:

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

These values collectively comprise the normative framework to be applied as a yardstick in this evaluation. Each of these principles will be evaluated in the following section.

# Object of evaluation: the OOP in European law and policy

## General functional description of the once-only principle

The DE4A project is organised against the policy background of the Single Digital Gateway Regulation. As the European Commission summarises the objective of the Regulation, “The single digital gateway will facilitate online access to the information, administrative procedures and assistance services that citizens and businesses need to get active in another EU country. By the end of 2020, citizens and companies moving across EU borders will easily be able to find out what rules and assistance services apply in their new residency. By the end of 2023 at the latest, they will be able to perform a number of procedures in all EU member states without any physical paperwork, like registering a car or claiming pension benefits.”[4].

DE4A principally, but not exclusively as will be explained below, targets the once-only principle enshrined in the Regulation. The Regulation describes this principle in recital 44 by noting that “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”.

DE4A is therefore 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.

DE4A (and the once-only principle as enshrined in the regulation) is therefore an example of **incremental innovation**: a form of innovation which builds on existing knowledge and aims at existing customers (as opposed to radical innovation, where either the knowledge, the usage, or both are at least partially new). As such, the principal challenge is to ensure that the innovations brought about by DE4A do not create ethical problems which were absent in the traditional way of working.

## Ethical implications – priorities for ethics evaluation

The DE4A project aims to explore implementations and usage of a technical system – i.e. an infrastructure – that would be required under the Single Digital Gateway Regulation to allow the ‘once-only’ principle to be respected. The usage of that technical system is limited to three specific pilot streams in DE4A: Studying Abroad, Doing Business Abroad, and Moving Abroad.

The DE4A infrastructure and the SDGR collectively allow existing national administrations to exchange existing information (evidence) in existing procedures. The central innovations of the SDGR and DE4A are that this exchange is done **electronically**, and that information should be exchanged **directly between administrations**, rather than simply providing documents to a citizen or company and requiring them to transfer the information to the relevant administration. As a result, citizens and businesses would no longer have to supply the same data to public authorities more than once, and 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.

There is however an additional element that impacts the ethics behind the SDGR and DE4A: as described in the Regulation, exchanges of evidence in principle must take place at the request of the user. Furthermore, the user must be shown a preview of evidence before it can be exchanged. These requirements act as safeguards that protect the user against unlawful exchanges, but they also imply that exchanges cannot take place without user intervention, even when this would be useful to protect the interests of the person concerned (e.g. to grant them access to benefits that they may be entitled to), the interests of third parties (e.g. to protect them against a person whose unlawful conduct could be detected and addressed if the relevant evidences could be easily exchanged), or even the interests of the public (e.g. to automatically detect fraud). Thus, there is a clear ethical choice that has been made, which focuses on user centricity and the voluntary choice to use the once-only principle only when this is in the interest of the user concerned.

There are exceptions to these rules where exchanges are explicitly permitted under national or European law without a prior request or preview, but based on the existing assessments in DE4A (notable in D7.1), these do not appear to be fully understood yet; and at any rate the standard (default) ethical choice of EU law and policy is to favour the interest of the individual user.

Taking these considerations into account, the principles and values outlined in section 2 can provisionally be evaluated as follows in relation to the once-only principle as envisaged by EU law and policy as a whole (without considering specific concerns for DE4A, which are outlined in the following section):

### **Dignity**, notably individuals’ right to be secure in their physical and mental integrity

**No particular risks** are likely to emerge. The DE4A infrastructure is intended to be used in existing exchanges of information between parties that are already sending/receiving that information. The change of modality of exchange is **unlikely to impact dignity** in any way, either negatively or positively.

### **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)

**While** **other freedoms are unlikely to be impacted negatively or positively, the right to data protection and privacy could be negatively impacted in the absence of sufficient safeguards.** The Regulation on the Single Digital Gateway already highlights this risk, and stresses that the technical system – and thus also DE4A’s infrastructure – must “comply with all applicable data protection rules, including the principle of data minimisation, accuracy, storage limitation, integrity and confidentiality, necessity, proportionality and purpose limitation. Its implementation should also comply fully with the principles of security by design and of privacy by design, and should also respect the fundamental rights of individuals, including those related to fairness and transparency” (recital 42).

In more concrete terms, the proposal requires that any exchange of personal data in the context of the technical system (and thus also DE4A’s infrastructure):

* Should take place only **upon prior request** of the end user (thus safeguarding lawfulness and transparency);
* Should take place only **after showing a preview of the relevant information** to the end user (thus safeguarding accuracy and transparency);
* Should **ensure the confidentiality and integrity, as well as a high level of security** of the exchanged information;
* Should be **limited to what is technically necessary** for the exchange of evidence, and then **only for the duration necessary** for that purpose (thus safeguarding necessity and storage limitation);
* Should not result in data being stored by the infrastructure longer than necessary **after showing a preview of the relevant information** to the end user (thus safeguarding accuracy and transparency);
* Should 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 safeguarding data minimisation and purpose limitation);

Thus, fundamental data protection principles are mandatorily protected by the Regulation. The main requirement for the DE4A project is therefore to design its infrastructure in such a way that all of these requirements are integrated and built into the infrastructure.

Compliance of these choices with European data protection law has been assessed by the European Data Protection Supervisor (EDPS) in its Opinion 8/2017 on the proposal for the SDGR[5], which generally evaluated these requirements favourably.

Separate WP7 deliverables in the DE4A project are dedicated to data protection, of which D7.1 Overview of legal and ethical requirements has been submitted thus far. We refer to this deliverable to examine details on the measures taken to ensure compliance with EU data protection law.

As is also highlighted in that deliverable, the General Data Protection Regulation, as the principal EU level legislation on the fundamental right to data protection, stipulates that a data protection impact assessment (DPIA) should be completed whenever a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons (article 35 of the GDPR). While the processing activities will be largely justified under the Single Digital Gateway Regulation, it is none the less **strongly recommended to conduct a formal DPIA** in order to assess precisely how these risks will be mitigated in practice.

The implementation of **the prior request and preview mechanisms** are important, since these are the main safeguards against negative impacts on European citizens and businesses, as are the potential further use of exchanged evidence for other procedures, since these can negatively impact users in a way that they cannot foresee. Finally, it is also important to opt for a **decentralised architecture in which no information about the end users is centrally stored**, since this otherwise creates a risk of systematic monitoring of citizens, profiling of their behaviour, and unlawful re-use of their personal data in a way that would be contrary to both the GDPR and the Single Digital Gateway Regulation.

In this way, privacy by design and privacy by default are embedded into the system architecture, in compliance with the requirements of the GDPR and the fundamental principles of Responsible Research and Innovation.

### **Equality**, including non-discrimination and rights of minorities and of societally more vulnerable parties

A potential risk is that the DE4A services would be accessible only to parties with adequate digital literacy and adequate digital infrastructure and connectivity, thus becoming a manifestation of the **digital divide** concern: some parties would benefit from DE4A due to their capability of working with a potentially complex IT system, whereas others would be left behind for reasons beyond their reasonable control. This would be particularly detrimental in the context of DE4A, since the exchanges relate to public sector services, and there would thus be a negative impact in citizens’ ability to satisfy legal obligations imposed by the government (either their own government, or in other Member States).

This concern is partially mitigated by the fact that use of the technical system should **not be mandatory, and that the users are permitted to submit evidence by means other than the technical system.** Thus, any accessibility concerns created by DE4A – which should of course be minimised – should not impair accessibility of the underlying governmental services, since citizens and businesses are always allowed to access those services without resorting to DE4A’s infrastructure.

Additionally, DE4A’s use cases cover **existing legally required exchanges,** which users would at any rate need to satisfy. In other words, DE4A will not result in an obligation to engage in an administrative procedure where none was required before. As such, all parties that would use DE4A would have needed to face the existing administrative burdens, and would receive DE4A as an additional alternative channel to satisfy and mitigate these burdens. They are free to use DE4A to satisfy these burdens more easily, or can use traditional channels if they perceive no sufficient benefits to DE4A.

None the less, these considerations do not exclude **the possibility that the digital services are inaccessible to some persons** (e.g. because the underlying process must be done digitally, is technologically complex, uses inaccessible formal language and so forth). This is an ethical concern, since the outcome may be that able persons are capable of satisfying procedural requirements more easily than less able persons, such as those who are less digitally literate. This creates a de facto inequality, since it places persons who already have clear benefits in an even more favourable position.

To a certain extent, this ethical issue is inherent to optional e-government services: as long as electronic services are only available upon request (as opposed to being used automatically whenever appropriate), inequality automatically occurs. The only structural way to resolve this problem would be to require once-only exchanges to *also* occur whenever this is possible and results in a benefit to the end user (even independently of any prior request); but this is not the policy option that was chosen by the Single Digital Gateway Regulation.

Nor is this likely to change in the near future; the recent Berlin Declaration on Digital Society and Value-Based Digital Government of 8 December 2020[6] noted that “*What is at stake is true digital empowerment of our citizens who want to benefit from a digitalised world. Everyone should be able to seize the opportunities offered by digitalisation. No one should be left behind”*, and that the Signatories of the Declaration “*Promote responsible and legally compliant re-use of data and the Once-Only Principle in line with the Tallinn Declaration and encourage new concepts such as personal data management based on user consent”* (emphasis added)*.* In other words: here too, the emphasis is on individual stewardship and choice, rather than on automatic exchanges. The choice is undoubtedly legitimate since it is the result of a balancing of interests, but it has negative ethical repercussions that require continued evaluation.

As a result of these factors, DE4A is **unlikely to have a significantly negative impact on equality,** provided that **accessibility of the design** is prioritised – in terms of technical user friendliness and complexity, as well as e.g. choice of language and guidance for users – and that appropriate support mechanisms are available to help such users who are unable to use the technical system.

### **Solidarity**, covering workers’ rights and labour rights, social security, collective bargaining, health care and environmental protection

**No particular risks** are likely to emerge. As the project creates no new information exchanges, nor eliminates them, the change of modality of exchange is **unlikely to impact solidarity** in any way, either negatively or positively.

### **Citizens' rights**, such as the right to vote, to proper administration, access to documents and freedom of movement

DE4A aims to implement the once-only principle in cross-border transactions, and can thus be seen as a way to **strengthen the right to proper administration**. The lack of a DE4A-like infrastructure in the EU today means that citizens and businesses must spend time and resources identifying legal evidentiary requirements, collecting the relevant documents, and providing them to any needed recipients. Each step creates the risk of errors and inefficiencies, which the once-only principle and DE4A aim to resolve. As such, DE4A should have a **generally** **beneficial impact on citizen’s rights.**

An important precondition is that the infrastructure is implemented and functions in a way that ensures its correct functioning, so that errors can be detected and addressed. In that light, in addition to what has already been stated above, it is important to ensure that **DE4A users are always provided with sufficient information to obtain assistance – including contact information from specific administrations – in case of any real or perceived problems.** Otherwise, the quality of administration may suffer when potential problems go undetected.

Furthermore, the aforementioned policy choice – namely that the once-only principle as envisaged in the SDGR is normally driven by user request and user approval – also implies that the principle is suboptimal in terms of ensuring proper administration. Since the exchanges of evidence are usually triggered by prior request and approval, there are three vectors where good administration suffers:

* Firstly, users who are unaware that they could benefit from online services will be unable to get any such benefit. Since they will make no request, no evidence will be exchanged, and they will either lose the benefit, or be required to take additional steps (such as paper procedures) to obtain the benefit to which they are entitled.
* Secondly, the legitimate interests of third parties (other than the users) are not taken into consideration. By way of example: a user may choose to refuse to use the technical system, because they know that current evidences will be unfavourable to them (e.g. because it shows that they no longer have a required accreditation). Instead, they can seek to submit outdated credentials outside of the technical system, allowing them to gain a benefit over a competitor that they should not have. In other words, the current user driven perspective on once-only allows users to continue to attempt to harm third parties if they desire to do so; the SDGR and the technical system in this case do not stop such behaviour.
* Thirdly, the societal interest in good governance is not optimally served, for the same reason: since evidence is in principle exchanged based only on the users request and approval, the once-only principle cannot be used to detect socially harmful behaviour (such as intentional fraud, or accidental but harmful non-compliance with legal requirements). The chosen user driven perspective on once-only therefore benefits individual interest over societal interest.

From these perspectives, the chosen approach of the **SDGR raises some ethical concerns on its ability to find an optimal balance between user interest, public interest and legitimate third party interests.** The choice made by the SDGR is certainly legitimate, but requires future evaluation in order to assess if the chosen balance is effective.

### **Justice**, including access to fair trial and effective remedy, and the right to defence.

**No particular risks** are likely to emerge. As noted above, DE4A aims to strengthen the quality and efficiency of public services, which, if done successfully, should reduce the need for legal redress in administrative proceedings where evidence was mismanaged. As such, DE4A should have a **beneficial impact on justice.** As noted above, this requires that the infrastructure operates correctly, and notably that **transactions are logged in a way that allows errors to be detected, evaluated and assigned to the responsible entity.** This is an important design requirement to ensure that the fundamental value of access to justice is not eroded.

# Object of evaluation - DE4A’s approach to the once-only principle and the SDGR

As was already highlighted above, DE4A mainly but not necessarily exclusively follows the logic and scoping of the SDGR. To the extent that it interprets the once-only principle in the same manner as the SDGR, all of the ethical evaluations and concerns of section 3 above also apply directly to DE4A in the same manner and to the same extent.

However, based on the currently consulted deliverables, DE4A is also contemplating to conduct certain piloting activities that exceed the exact limitations of the SDGR. Part 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 the SDGR, as is explored in D7.1 Overview of legal and ethical requirements. To the extent that such models would actually be piloted (this is still a topic of discussion at the time of reporting), the ethics evaluation would be impacted, notably in relation to:

* **Data protection,** which could be negatively impacted. The prior request and preview were considered to be fundamental safeguards in relation to data protection, privacy and confidentiality (among other objectives). If these would be weakened or removed, data protection risks would inevitably increase. In this case, a DPIA identifying and assessing these risks and potential mitigating measures would be critical.
* **Equality and good governance,** which could be positively impacted. The evaluations above precisely highlighted the ethical risk that the request and preview requirements could result in less able persons losing benefits that they would be entitled to, and that the quality of governance could suffer as a result of harmful behaviour not being optimally detected. Push models and subscription models could ameliorate these concerns.

Furthermore, other ethical concerns could arise in relation to the use of more innovative technologies with transformative impact, notably blockchain and machine learning. Insofar as these are only used to improve effectiveness, user friendliness and accountability, no new ethical challenges need to arise. However, if such technologies are used to constrain or steer (nudge) user behaviour, further ethical problems occur. At these stage however, there is no indication that such functional choices would be made. This issue will be monitored in future reports, but there is no *prima facie* concern on these topics.

As was already noted above, this report will not assess the ethics behind the use cases of DE4A as such (Studying Abroad, Doing Business Abroad, and Moving Abroad). It assumes that existing Member State and EU laws and policies relating to cross border mobility are ethical, or at least that the ethics behind these laws and policies do not require assessment within DE4A.

# Conclusions

Based on the ethics assessment, the current actions and plans of the DE4A project are in line with the EU’s ethical requirements.

Two ethical challenges are however identified which should be monitored and evaluated as priorities in the reminder of the project:

* **Data protection**. While the Single Digital Gateway provides a fundamental data protection constraints, it is not certain at this stage whether all DE4A piloting activities will remain strictly within the confines of that legislation. In addition, implementation choices made within DE4A can affect the quality of data protection for citizens, even when remaining within the confines of the Regulation. A DPIA would be strongly recommended to mitigate data protection challenges.
* **Equality and citizen’s rights, including the right to good administration**. The Single Digital Gateway Regulation promotes user request and preview as basic requirements, which protects citizens and businesses against breaches of privacy and confidentiality. As a trade-off however, the benefits of the once-only principle are only available to digitally literate persons who are capable of requesting it, and individual interest takes precedence over societal interests. It is recommended to explore what the implications are, and to evaluate whether this policy choice is ethically optimal.

Further compliance with these requirements will be evaluated in the future Ethics Reports.

References

1. DE4A Description of the Action
2. Responsible research & innovation Guidlines. <https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation>, retrieved on 2020-12-17
3. Value Sensitive Design and Information Systems, BATYA FRIEDMAN, PETER H. KAHN, JR., AND ALAN BORNING. <https://vsdesign.org/publications/pdf/non-scan-vsd-and-information-systems.pdf>, retrieved on 2020-12-17
4. The single digital gateway. <https://ec.europa.eu/growth/single-market/single-digital-gateway_en>, retrieved on 2020-12-17
5. EDPS Opinion 8/2017 on the proposal for a Regulation establishing a single digital gateway and the ‘once-only’ principle, 1 August 2017. <https://edps.europa.eu/sites/edp/files/publication/17-08-01_sdg_opinion_en.pdf>, retrieved on 2020-12-17
6. Berlin Declaration on Digital Society and Value-Based Digital Government of 8 December 2020. <https://www.bmi.bund.de/SharedDocs/downloads/EN/eu-presidency/berlin-declaration-digital-society.pdf;jsessionid=16E411E2A284D84BDE5A1956E1439F1D.2_cid364?__blob=publicationFile&v=2>, retrieved on 2020-12-17