D5.3

Overview of Legal Landscape and Regulations

Project number:	959072
Project acronym:	mGov4EU
Project title:	Mobile Cross-Border Government Services for Europe
Start date of the project:	1st January, 2021
Duration:	36 months
Programme / Topic:	H2020-SC6-GOVERNANCE-2020, Governance for the future

Deliverable type:	Report
Deliverable reference number:	DT-GOVERNANCE-05-959072 / D5.3 / V1.1
Work package contributing to the deliverable:	WP5
Due date:	December 2021 – M12
Actual submission date:	30th May 2022

Responsible organisation:	TLX
Editor:	Hans Graux
Dissemination level:	PU
Revision:	V1.1

Abstract:	A key requirement for mGov4EU is that the project is executed in full compliance with applicable legislation, including the GDPR, SDGR, and the eIDAS Regulation. This deliverable summarises the applicability of these legal frameworks and identifies the principal consequences for the project.
Keywords:	Legal, GDPR, SDGR, eIDAS, once-only

The project mGov4EU has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 959072.

Editor

Hans Graux (TLX)

Contributors

Mahault Piéchaud Boura (TLX)

Disclaimer

Executive Summary

The mGov4EU project aims to provide the means to fully integrate mobile devices into European public sector applications. Beyond technical and functional requirements, one of the main challenges is ensuring that European and national legal requirements are considered in the design of the architecture and that they are taken into account during piloting.

This is not a trivial problem to resolve, due to the breadth of the legal framework, its complexity, and the fact that it is changing and evolving continuously. In this deliverable, we provide an inventory of the legal landscape, and describe applicable regulations. We examine their impact on the mGov4EU pilot activities in terms of drivers and barriers.

The deliverable explores four legal topics in particular:

- Privacy and data protection, i.e. the ability to ensure that mGov4EU's architecture and components satisfy the requirements of EU data protection law, in particular the General Data Protection Regulation (GDPR), in accordance with the principle of privacy by design; and that they can ensure a high level of data protection for its users;
- E-government and public services, i.e. the capability of mGov4EU to be integrated into public sector applications, taking into account, in particular, the existing and emerging legal framework related to European cross-border once-only information exchanges in the context of the Single Digital Gateway Regulation (SDGR).
- Identification and authentication, i.e. the capability of mGov4EU to reliably identify its users, and to ensure that the integrity and authenticity of any exchanged information can be determined, e.g. by relying on electronic signatures and/or electronic seals as defined in the Electronic Identification and Authentication Services Regulation (eIDAS Regulation). This should also take into account ongoing discussions in the context of a potential amendment of this Regulation to create a legal framework for a European Digital Identity Wallet – a particularly relevant topic for mGov4EU;
- Governance and sovereignty, i.e. the ability of mGov4EU users to be able to retain sufficient control over their data, including by determining who receives it, for what purposes they may use it, and by ensuring that the information cannot be captured or abused with the mGov4EU architecture itself. This issue is presently not regulated (beyond the provisions of the GDPR related to data subject rights), but the proposed Data Governance Act (DGA) will be briefly explored as a potentially relevant topic.

After identifying the relevant requirements, the pilot use cases are summarily examined based on the available information; and the impact of the requirements on the mGov4EU architecture is examined.

As will be shown below, mGov4EU is designed to comply with the relevant legal frameworks and has the ability to significantly advance the state of the art due to its focus on mobile applications and services.

The following table summarizes the relation of D5.3 to other tasks, work packages, and deliverables:

Table 1: Relation to other mGov4EU work packages, tasks, and deliverables

Contributing tasks of this WP:	T5.4
Input from other tasks/WPs:	-
Output to other tasks/WPs:	T5.3, T6.1
Output to other deliverables:	D6.2

Table of Content

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Meaning
AI	Artificial Intelligence
CA	Consortium Agreement
DPIA	Data Protection Impact Assessment
DoA	Description of Action
Dx.y	Deliverable number y, belonging to WP number x
DGA	Digital Governance Act
EC	European Commission
EDIW	European Digital Identity Wallet

Abbreviation	Meaning
EEA	European Economic Area (comprising all 27 Member States, Iceland, Liechtenstein and Norway)
eIDAS	eIDAS Regulation
GA	Grant Agreement
GDPR	General Data Protection Regulation
IPFS	Interplanetary File System
KPI	Key Performance Indicator
Mx	Month X
NIS	Network and Information Security
PC	Project Coordinator
PM	Person-month
QA	Quality Assurance
QM	Quality Manager
RASCI	Responsible/Accountable/Supportive/Consulted/Informed
RP	Reporting Period
SDG	Single Digital Gateway
SDGR	Single Digital Gateway Regulation
TL	Task Leader
UC	Use Case
WP	Work Package
WPx	Work Package number x
YRx	Year X

Chapter 1 Introduction

1.1 Purpose

This deliverable is drafted in the context of Task 5.4 - Assessing the Legal Landscape and Regulations. This task focuses on the identification of legal drivers and barriers for the implementation and application of cross-border government services on mobile devices in light of the SDGR and the once-only principle. These drivers and barriers result at the European Union (EU) level principally from the GDPR in relation to the protection of personal data (such as the need for lawfulness, proportionality, and privacy by design, among others), and from the eIDAS Regulation (EU) 910/2014, on the validity of electronic documents and requirements for trustworthy identities. However, national constraints need to be identified as well, to determine pilot specific possibilities and constraints (e.g. requirements to anonymise or pseudonymise personal data in a certain manner, requirements to complete certain agreements or to obtain certain permissions to collect or analyse the data, or any data localisation requirements).

Functionally, this report aims to identify the legal barriers and drivers for the implementation of the mGov4EU system and the pilots aiming to demonstrate it. To that end, it is important to identify applicable legal requirements while the system and pilots are still being defined, to ensure their intake into the design process. In terms of outcome, this deliverable aims to detail the legal requirements related to a functional mGov4EU solution, considering data protection, electronic identification, and once only principles policies areas.

Since the pilots are not yet fully defined at the present stage, the analysis of national requirements is limited in the present iteration of the deliverable. This deliverable will be iteratively refined and adjusted as the pilots evolve, to ensure that all relevant requirements are taken into account.

1.2 Methodology

This deliverable briefly summarises the main elements of the overall mGov4EU system and its general architecture, and briefly discusses the pilots. On that basis, it identifies the policy areas that should be included in the assessment and assesses their relevance to the system. More in detail:

- This deliverable first identifies the characteristics of the mGov4EU system, as they are presented in the Description of Action and the existing deliverables describing it (notably D1.2 Specification of Reference Architecture and D1.3 Specification of System Requirements), as well as the current description of the pilots and demonstrators prepared by the consortium. Then, this deliverable identifies the policy areas relevant to the action of the mGov4EU.
- In a second step, the policy areas and any relevant legislation are further defined and analysed, and legal requirements are identified. This deliverable does not aim to present an exhaustive description of every piece of legislation applicable to the mGov4EU system. Rather, after of general introduction of the main elements of each policy area, as well as anticipated regulatory changes, this deliverable presents, in the form of a table, a series of requirements that should be considered for the design, selection of components, and implementation of the system.
- In a third step, the identified requirements are applied to the pilots. For this last stage of the assessment, it should be considered that not all piloting details have been fully settled at the time of submission, and that they are still subject to evolution. Where mGov4EU components rely on existing solutions that have been designed specifically to implement diverse EU policies or laws (e.g. the Connecting Europe Facility (CEF) Building Blocks elaborated in the context of the eIDAS Regulation), compliance with EU legal requirements can be reasonably assumed, and no new compliance verification is done.

Chapter 2 Summary description of the mGov4EU system and relevant policy areas

2.1 mGov4EU purpose and approach

The purpose of the mGov4EU project is to develop an ecosystem for secure mobile government services to be used across Europe, implementing the principle of mobile-first, according to which e-government principles should be as available as possible from a mobile device.

2.2 Broader policy context

From a legal and policy perspective, that implies that mGov4EU builds on the background of the 2017 Tallinn E-government Declaration, which emphatically supported digital-by-default as a foundational policy principle. In the Declaration, Members States committed to:

- *provide citizens and businesses with the option to interact digitally with public administrations, if they choose to, […]*
- *take steps to reduce the need for citizens and businesses to unnecessarily interact with public administrations, for example, by relying on (re)use of data;*
- *take steps to further increase the readiness of citizens and businesses to interact digitally with public administrations by developing their digital skills as well as promoting the available digital public services (including cross-border ones);*
- *[…]*
- *ensure better digital accessibility of public services and information for all citizens and businesses, including by improving the accessibility of public administration websites and mobile apps.*

Thus, the Tallinn Declaration focuses strongly on mobile, user-driven once-only exchanges as a pillar of future e-government policy.

Secondly – and related to the Tallinn Declaration - mGov4EU also builds on the recently adopted SDGR, which creates the legal framework for cross-border once-only data exchanges, albeit without a focus on mobile infrastructure. As a result of the SDGR, Member States must ensure that certain administrative procedures enumerated in the Regulation (as will be described below) can be completed electronically by the end of 2023, including in cross border situations. During such electronic procedures, the relevant public administrations must exchange relevant evidentiary documents directly between themselves, rather than relying on the citizen to act as a courier between administrations, as is often the case in analogue procedures.

Thirdly, and again connected to the Tallinn Declaration, the eIDAS Regulation provides a legal underpinning for the mutual recognition of electronic identification schemes between public administrations in 2014, and also created harmonised legislation for certain trust services, including electronic signatures. This has been a great enabler for European digital transactions, which has been further supported by the development of shared European infrastructure to build applications and services, such as the CEF building blocks. The eIDAS Regulation however lacks a specific emphasis on mobile services, and this too was an element that was highlighted in the Tallinn Declaration: Member States should "*work to increase the uptake of national eID schemes, including to make them more userfriendly and especially more suitable for mobile platforms, while ensuring their appropriate security levels".* As will be discussed in the sections below, this intention has been followed up in the EU through a new regulatory initiative, specifically a proposed amendment of the eIDAS Regulation that would create a specific legal framework for European Mobile Identity Wallets.

mGov4EU combines these influences and aims to create a trustworthy federation of collaborative platforms, which facilitates the co-delivery, reuse, and trustworthy provision of accessible and easy-

to-use public services, implementing the once-only, digital-by-default and mobile-first principles in a user-centric and user-friendly manner, combining and enhancing the existing eIDAS layer (for electronic identification and electronic signatures) and SDGR layer (for cross border once-only services) with sufficiently flexible modules for mobile devices to be re-used in the emerging and thus still heterogeneous European mobile-government landscape.

2.3 High-level overview of the mGov4EU system architecture

Before summarising the main legal frameworks, it is important to bear in mind the general mGov4EU architecture. This is developed mainly in WP1, and is described in great detail in D1.2 Specification of Reference Architecture. Here, we will mainly summarise the general concepts and principles, as captured in **Fehler! Verweisquelle konnte nicht gefunden werden.**:

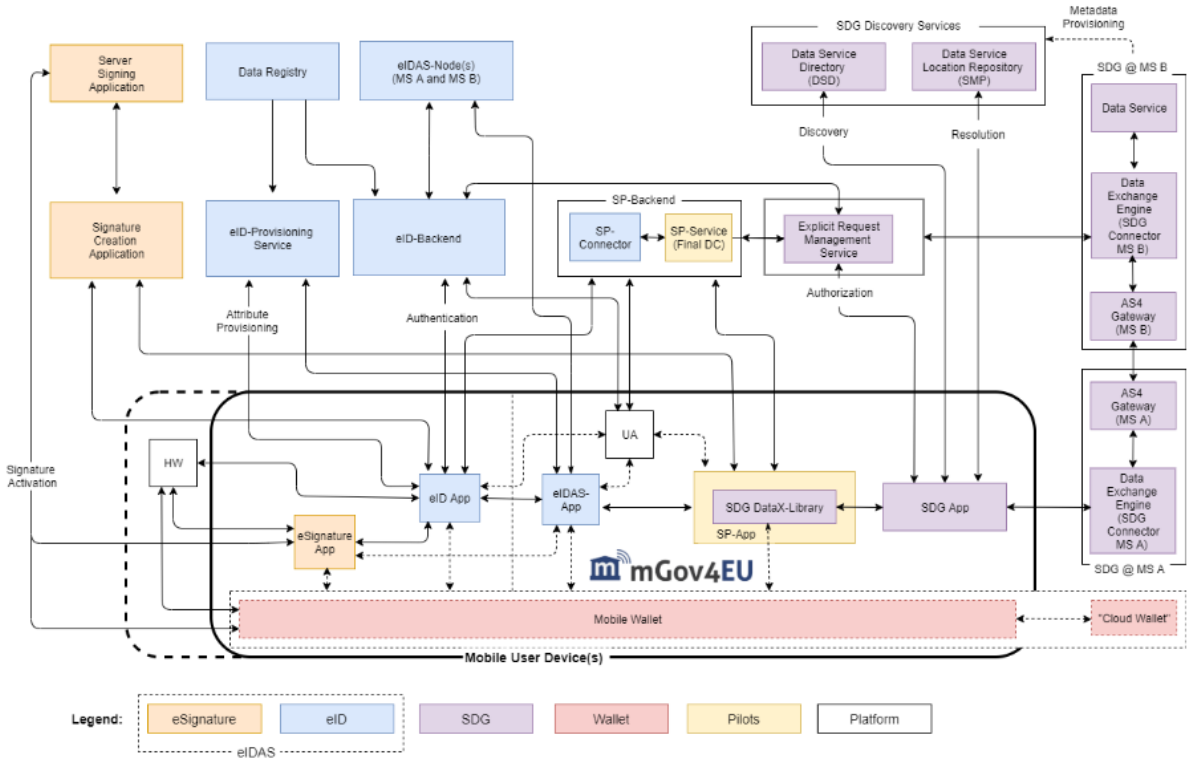

Figure 1: mGov4EU – Reference Architecture at a glance, as defined in D1.2

As **Fehler! Verweisquelle konnte nicht gefunden werden.** shows, the eSignature, eID, and SDG components of the mGov4EU architecture rely on components that do not originate from the mGov4EU project. These components were largely developed either in the framework of the CEF (for the eSignature and eID components in **Fehler! Verweisquelle konnte nicht gefunden werden.**), or they are currently being developed by the European Commission in order to ensure the correct implementation of the SDGR (for the SDG components in **Fehler! Verweisquelle konnte nicht gefunden werden.**). These components, marked in orange, blue and purple in the graphic above, are thus created and maintained externally from mGov4EU, and are part of the legal assessment only where the mGov4EU components interact with them.

In contrast, the Mobile Wallet and Pilots components will be developed specifically for the purpose of the mGov4EU project. They will bring together:

- an eID app, which is the local component necessary to activate the eID protocol;
- an eIDAS app to integrate the mGov4EU system with the eIDAS nodes of the EU Member States;
- an eSignature app to support eSignature generation at the initiative of the user;
- and interfaces to SDG components (as will be discussed below) through an SDG app.

Therefore, this deliverable focuses on the identification of requirements that apply to these unique and new elements.

For the avoidance of doubt, it is noted that mGov4EU is aware that the Commission and the Member States also aim to jointly develop specifications and potentially reference implementations of the European Digital Identity Wallet. As will be discussed below, this is currently being examined in the context of the so-called eIDAS 2 Proposal, and the outcome may be that the Wallet becomes a CEF building block in the future. However, such specifications or reference implementations are presently not yet available, and therefore mGov4EU has a unique opportunity of advancing the state of the art in a way that complies with the main legal requirements, as discussed below.

2.4 Identification of relevant legal frameworks to be included in the assessments

The main characteristics and objectives of the mGov4EU infrastructure have been summarily described above. Based on those elements, four legal areas will be examined in detail in this deliverable (see **Fehler! Verweisquelle konnte nicht gefunden werden.**):

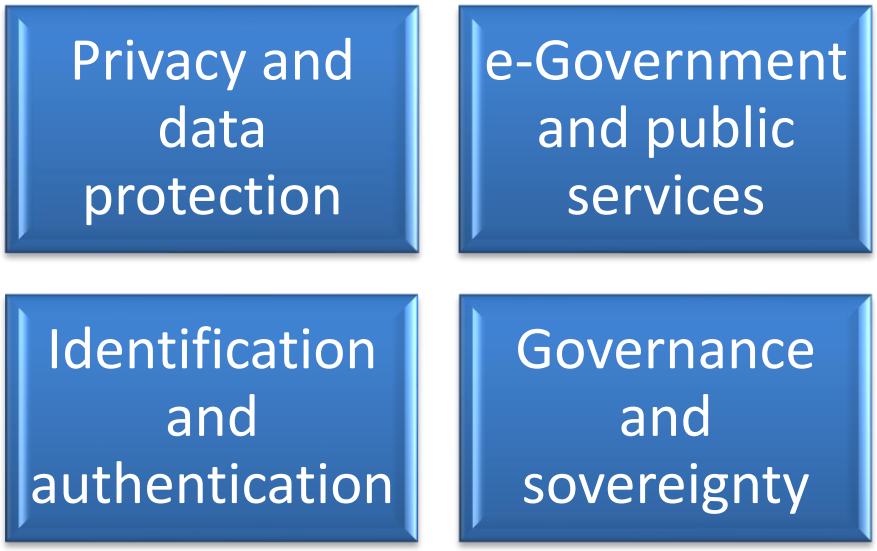

Figure 2: mGov4EU – Overview of relevant legal frameworks

More specifically:

- **Privacy and data protection** is a central requirement for the mGov4EU infrastructure since one of the principal benefits and drivers behind a mobile ecosystem is that it gives users control over their data, without relying on third-party storage providers. Taking into account that users in this project are always natural persons, information relating to them will be qualified as personal data, as defined under EU law. The platform thus needs to be designed with privacy and data protection in mind, in accordance with the privacy by design and privacy by default principles of European data protection law, notably the **GDPR**.
- **e-Government and public services** are the second key vector. While mGov4EU doesn't need to be used exclusively for public sector use cases, its use in public sector applications is an explicit target, as envisaged in the **SDGR**. With that in mind, this legal framework needs to be assessed too, to ensure fitness for purpose.
- **Identification and authentication** are a cross-cutting – i.e. non-sector specific and non-use-case specific – requirement. For the mGov4EU infrastructure to be useful, the users have to

be identifiable. Moreover, any information that they make available via mobile applications must be shared in a way that allows integrity and authenticity to be ensured appropriately. In this context, 'integrity' implies the ability to verify that information hasn't been modified or corrupted; and 'authenticity' implies the ability to link information to a specific source. In this way, the recipient can determine to what extent the information can be trusted. Thus, mGov4EU must comply with the **eIDAS Regulation**, and should take into account the recently published proposal for amendment of this Regulation.

- **Governance and sovereignty** finally refer to the ability of users to keep control over their data, on the one hand by ensuring that data on their mobile device cannot be directly abused by third parties, and on the other hand by integrating the ability for citizens to exercise their rights towards third parties. This is driven by the **GDPR**'s provisions on information security and data subject rights, but inspiration will also be sought in the control provisions of the **SDGR** and the recently proposed **Data Governance Act (DGA).**

The principal legal frameworks at the EU level are thus the GDPR, SDGR, eIDAS Regulation (and the proposed amendment), and the DGA proposal. Each of these will be briefly discussed in the sections below, before proceeding to a more structured analysis in Chapter 3.

2.4.1 Privacy and data protection

The most direct purpose of mGov4EU is to allow citizens to perform administrative acts directly from a mobile device. Since this inevitably requires the processing of that citizen's personal data, the EU framework relating to the protection of personal data is fundamental. For mGov4EU's piloting activities, in particular, it is worth noting that they all target natural persons exclusively: while the SDGR's public services scope also includes procedures that target companies (or other types of legal entities), mGov4EU focuses only on natural persons; hence the importance of data protection as a fundamental right in the EU.

However, data protection is only one aspect of privacy, and vice versa. Privacy in general protects the private sphere of natural persons. Hence, the more fundamental norms found in the EU Charter for Human Rights, notably its provisions on the right to respect for private and family life (Article 7) next to the respect for data protection rights (Article 8) are relevant too and should guide the principles implemented in the framework of mGov4EU.

According to the European Union Charter of Fundamental Rights, which must be followed in the implementation of the EU policy, everyone has the right to the protection of their personal data. Furthermore, such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law (such as a contractual relation or a legal obligation). Everyone has the right of access to data that has been collected concerning them, and the right to have it rectified, as well as to oppose or limit their processing, among others.

More detailed rules are set out in the 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 (General Data Protection Regulation or GDPR). The GDPR enables EU residents to have better control over their personal data. It harmonises the framework for the processing of personal data across the EU, and implements a single and largely uniform set of rules for all businesses and other entities processing personal data across the EU, and even beyond (when they process EU citizens' data).

Next to the GDPR, the privacy of electronic communications is explicitly protected by the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications – ePrivacy Directive), as amended in 2009. This Directive governs the exchange of information through public electronic communication services such as the internet and mobile and landline telephony and via their accompanying networks. These services and networks require specific rules and safeguards to ensure the users' right to privacy and confidentiality.

From a pure data protection perspective, mGov4Eu can be approached and analysed as a Personal Information Management System (PIMS). PIMS are designed to help individuals manage and control their personal information, including personal data. Within a PIMS, the user is the one holding and managing the information, including information exchanges.

As described in greater detail in a 2021 TechDispatch published by the European Data Protection Supervisor, a fundamental feature of PIMs is their capacity for the user to visualise who (which organisation) accessed their information through access controls and access trail features. Users may choose the data available to third parties and set access criteria. Usual features of PIMS also include data storage and data transfer.

Given those core functionalities, mGov4EU meets the fundamental criteria of a PIMS. mGov4EU user components will be installed on the user's mobile device as a wallet enabling the use of various services (governmental but also private), using Member States eID schemes, and sometimes interacting with the Single Digital Gateway. The mGov4EU wallet will enable its user to easily identify themselves and manage their information storage and exchanges via the apps. In that perspective mGov4EU can be construed as a PIMS.

There are multiple specific data protection issues associated with PIMs, as highlighted also in the aforementioned TechDispatch:

- Data protection by design and by default are principles that underpin the whole GDPR. Data protection must be considered already during the conception of the services and included in the design. This also means that effective data protection must be an automatic result of the use of the service. Data protection by default supposes that the default settings of the services, which of course may be later customised by the user, must ensure the highest possible protection of the personal data of the user out of the box, i.e. without user configuration
- Consent management: PIMS' most interesting feature is to enable users to manage their data, and grant access to it for various purposes. This supposes that a user can consent to the processing of personal data by third parties (by allowing them to receive and use it for specified purposes), but also that they should be able to withdraw their consent just as easily. Therefore, a PIMS must have a user-friendly and intuitive consent management system, thus supporting user control over their personal information. As will be explored further below, there are instances, however, where the processing of personal data cannot be based on the consent of the data subjects, but relies on other legal bases, such as legal obligation or performance of a contract. At any rate, the data subject must be adequately informed and have the possibility to object to the processing of their personal data.
- Transparency and traceability: PIMS support the traceability and transparency of the processing of the user's personal information, and thus support trust in the use of e-government solutions implemented by administrations.
- Data portability, interoperability and accuracy of the data: the data provided through PIMS are primarily managed by the users, who are well-positioned to ensure the veracity and accuracy of their personal data. This is another feature that supports data protection. PIMS also inherently offer metadata and data in machine-readable format, thus supporting their portability and mitigating lock-in risks.
- Data security is a fundamental aspect of data protection. In the framework of PIMS, the security and confidentiality of data must be fully ensured both for data at rest (i.e. on the mobile device) and in transit (i.e. while obtaining it from information providers to load it onto the phone; and while sending it to service providers), supporting data encryption and enhancing the minimisation of data (i.e. avoiding needless retention and storage of unnecessary data).
- The rights of access, rectification, and erasure: some data subject rights set in the GDPR can be exercised directly by the user through a PIMS, as they have direct access to the data. Depending on the configuration and capabilities of a PIMS, it can e.g. be used to identify who has received data via the PIMS and retain relevant contact information, so that rights requests can be provided directly in a standardised manner. As always however, the

existence of a rights support interface doesn't mean by definition that the rights requests will be successful. By way of a simple and intuitive example: if a PIMS was used to provide data to tax authorities, the PIMS will typically not allow a user to demand that the tax authorities delete their data or that they stop using it. In this case, there is a legal mandate for the tax authorities that overrides the citizen's individual request.

Clearly, requirements emanating from the GDPR must be identified and respected at all times in mGov4EU.

2.4.2 E-government and public services

While mGov4Eu has a broader role as a system for managing personal data and controlling information flows, mGov4EU particularly also aims to act as an intermediary tool between citizens and public administration for the provision of public services. In that context, it should be capable of supporting and/or contributing to information management as prescribed by relevant EU legislation, such as the Single Digital Gateway Regulation and its forthcoming implementing act. While the mGov4EU system is not intended to be used solely by public administrations, it should support actors relying on it by providing a system that is SDGR compliant by design.

The SDGR is a broad legislation, that envisages the creation of a Single Digital Gateway (SDG). The SDG is designed to facilitate online access to the information, key administrative procedures, and assistance and problem-solving services that citizens and businesses may wish to contact if they encounter problems when exercising their internal market rights while living in or doing business in another EU country. As a component of the SDR, the SDGR also envisages the creation of a 'technical system', as will be further described in the sections below, which can be used by competent authorities in the Member States to directly exchange digital information (so-called evidence) that is relevant and required to support certain public services listed in the SDGR.

In order to be useful for SDGR procedures, the mGov4EU system, therefore, needs to comply with the SDGR and its functional requirements, not in the sense that it needs to *be* the technical system that's defined in the SDGR – this system is created by the Commission and the Member States outside of mGov4EU – but rather in the sense that mGov4EU components must be capable of *interacting* with the technical system in a trustworthy manner, as envisaged by the SDGR. In that way, mGov4EU progresses the state of the art, since formal SDGR initiatives presently do not focus on mobile e-government.

2.4.3 Identification and authentication

Identification and authentication are transversal requirements going beyond the concept of mGov4EU. Identification and authentication of users and information in public services users is a fundamental cross-cutting issue. Given the purpose for which the mGov4EU system is intended to be used, reliable and legally compliant identification and authentication are paramount. These rely on the integrity and authenticity of any information managed by or shared though the mGov4EU system.

This topic is regulated principally in the EU by the eIDAS Regulation. This piece of legislation aims to improve trust in EU-wide electronic transactions and to increase the effectiveness of public and private online services and e-commerce. It broadly covers three topics, all of which are relevant to mGov4EU:

- Firstly, it provides a legal framework for the mutual recognition of electronic identification schemes, including means of identification issued to persons under that scheme. The recognition requires prior notification by Member States (i.e. Member States have to inform the Commission and each other of the schemes and their characteristics), as a result of which (after assessment and publication) the schemes can be used to access public sector services in other the Member States.
- Secondly, it creates a legal framework for certain trust schemes, including electronic signatures and electronic seals. These can be provided by specialised market actors (so-called trust service providers), who are subject to supervision at the national level. The

highest quality trust services (so-called qualified trust services) must be audited by independent specialised bodies, and their status is published online, so that the legal value of their services is readily apparent across the EU.
- Thirdly, it establishes a summary non-discrimination principle for electronic documents, stating that electronic documents cannot be denied legal value or validity merely on the grounds that they are in an electronic form.

Given that mGov4EU is intended to be usable across the EU, it is vitally important that it supports the eIDAS framework, specifically by ensuring that identification through the app allows an assessment of whether the eID credentials are based on an eIDAS notified identity; and that it allows the creation of qualified electronic signatures by the users.

The eIDAS regulation dates back to 2014, and is not particularly focused on mobile ecosystems. While the use of mobile devices is not prohibited – neither for electronic identification nor for electronic signatures – and in practice the market already provides mobile-based solutions, the eIDAS Regulation contains no specific rules on mobile identification, mobile signing, or mobile data governance systems. However, in June 2021 the Commission approved a proposal for a regulation amending the eIDAS regulation in order to establish a framework for a European Digital Identity. Among other interesting innovations, the proposal aims to introduce European Digital Identity Wallets, defined as products and services allowing users to store identity data, credentials and attributes linked to their identity, to provide them to relying parties on request and to use them for authentication, online and offline, for a service, and to create qualified electronic signatures and seals (Article 1.3 (i) proposed European Digital Identity Regulation).

The European Digital Identity Wallet could be used, for example, to open a bank account, share digital documents, or prove a specific personal attribute, such as a medical certificate or professional qualification. The Member States would be required to ensure the availability of at least one type of Wallet for its citizens, although citizens are free to decide whether they want to have or use such a Wallet or not.

Obviously, the eIDAS 2 proposal (as it is sometimes called) is directly relevant to mGov4EU. One of its objectives is after all to allow citizens to manage their own data via a mobile wallet. The mGov4EU app ecosystem could easily be used as a building block for such a wallet. Depending on piloting results, mGov4EU might end up building a prototype implementation of such a wallet. For that reason, mGov4EU should consider the requirements of the eIDAS 2 proposal, even though it is currently still just a proposal. In that way, the mGov4EU apps can be used as inputs or as lessons learned for the eIDAS 2 Wallet.

2.4.4 Data governance and sovereignty

Data governance and data sovereignty, in the context of mGov4EU, refer to the ability of the citizen to manage their own data and to keep control of it. There is no single legislation that directly addresses this topic; but as a policy area the concept is supported by the GDPR, the SDGR, and the upcoming Data Governance Act (DGA). More specifically:

- The GDPR defines certain data subject rights, i.e. rights that a person can exercise in relation to their personal data, in order to support their reasonable control over their data and the use thereof. These include the right to transparency (including the right to obtain a copy of their personal data processed by others), the right to have their data corrected or deleted, and the right to oppose certain forms of processing of their data. All of these rights are subject to constraints, exceptions and conditions - e.g. citizens usually cannot stop governments from processing their data in the context of public interest tasks; and governments will normally require strong proof of identity before granting data subject rights. Nonetheless, the GDPR's approach to data subject rights is a powerful enabler of personal data sovereignty, to which mGov4EU could usefully contribute.
- The SDGR contains further safeguards, which of course by definition formally only apply in the context of SDGR procedures (i.e. in the context of certain explicitly listed e-government services, thus excluding any purely private sector applications). Nonetheless, these safeguards can be universally adopted and applied in mGov4EU, irrespective of the use

case, in order to ensure that best practices that strengthen the citizen's control over their data are consistently applied. The two main principles in the SDGR in this respect are the requirement that data cannot be shared without an explicit prior request from the user, and that the user must always be able to preview data before it can be shared with a recipient, so the user can block transfers that are incorrect or harmful to their interests. These requirements can be applied as general principles in mGov4EU, thus strengthening sovereignty.

- Finally, the DGA proposal covers several topics. This proposed piece of legislation aims to make public sector data more broadly available for re-use; to enhance sharing of data among businesses; to allow personal data to be used with the help of a 'personal data-sharing intermediary', designed to help individuals exercise their rights under the GDPR; and finally to facilitate data use on altruistic grounds. For mGov4EU, mainly the third topic (the personal data-sharing intermediary concept) is useful. It cannot be directly applied to mGov4EU without modification, because as the concept suggests, it requires an intermediary – an independent not-for-profit entity that governs data sharing activities, in interaction with the user. mGov4EU on the other hand is architecturally decentralised: there *is* no central intermediary that holds the user's data, and that governs it on their behalf. The mGov4EU approach is (arguably) more empowering, since it allows data to be retained by the user themselves, on their own mobile devices, and deciding independently when and on which grounds data can be shared, and with whom. Nonetheless, there are fundamental safeguards imposed by the draft DGA – notably the requirement that data cannot be shared, monitored or commercially exploited without user consent.

More detailed requirements analysis will be done in Chapter 3 below. However, this analysis would not be able to adequately consider requirements that are specific to each pilot. For that reason, the currently envisaged use cases and piloting scenarios are described below, including an initial assessment of relevant policy topics, legal frameworks, and specific considerations.

2.5 mGov4EU use cases and piloting scenarios

The mGov4EU system will be demonstrated through three use cases. These will be briefly described below from a functional perspective. As noted above, these are presently still under discussion, and will not be fully finalised until month 18, as scheduled in the Grant Agreement. For that reason, a high-level perspective is taken only, focusing mainly on potential legal challenges.

2.5.1 I-Voting pilot: online voting supporting institutional consultation

The purpose of this pilot is to demonstrate the feasibility of using the mGov4EU apps for the authentication of the voters using their electronic national identifiers and national eID schemes, and evaluate the solution in terms of usability, efficacy and security.

The current planning is for this functionality to be tested through a consultation of international students of the UTartu University in Estonia. Students will be able to register to vote via the mGov4EU App, through which they will be able to identify themselves. eSignature functionality is also under consideration: if piloted, and if the users' national eIDs support it, they will also be able to sign the ballot cast to ensure it has been cast by an eligible voter.

For the avoidance of doubt, it is not envisaged that the pilot is tested in the context of a public political election (e.g., legislative or presidential elections). While this would functionally also be possible, it is not presently retained as a use case, and therefore national public political election laws do not apply. It will still be assessed whether the specific use case is subject to Estonian laws (or bylaws of the University); this depends on the definition of the scope of the vote, which has not been finalised yet.

Nonetheless, certain features create new legal questions:

- The first functional goal of the iVoting use-case is the use of a unique electronic national identifier. This creates data protection challenges, since data minimisation features are

needed to ensure voting does not facilitate user profiling (by linking behaviour across different contexts on the basis of the identifier). The data minimisation principle therefore needs to be rigidly adhered to. Moreover, in a student context, relying on the consent of the students is not trivial, since their consent may not be legally valid: if they may have the impression of being coerced to vote, consent is not free, and therefore does not satisfy the requirements of the GDPR. Depending on the chosen voting use case (i.e. who votes and what they are voting on), there is likely to be a separate legal basis, such as the legislation governing the operations of the university.

- Moreover, the pilot should support a link to the eIDAS Regulation: while the pilot does not legally require the use of EU level notified eID schemes under the eIDAS Regulation, elections require that only eligible voters vote and that it is possible to ensure uniqueness of voting: identities must be validated with sufficient assurance that no single person can vote twice or more.
- As an optional functional goal, the demonstrator is considering implementing a signature that either builds on the eIDAS rules for qualified electronic signatures (thus fully satisfying the eIDAS Regulation's requirements on this point), or that could rely on the electronic national identifier of an eIDAS notified identity to demonstrate the authenticity of the ballot cast (resulting in a non-qualified electronic signature). Either way, an assessment is needed relating to eIDAS e-signature requirements.
- Finally, as another optional feature, the demonstrator could rely on the SDG to obtain validation of voting rights. This would require the implementation of the SDG requirements.

2.5.2 Smart mobility pilot: state-subsidised mobility services requiring identification and authentication

The goal of the Smart Mobility Pilot is to demonstrate the suitability of the mGov4EU infrastructure for innovative state-subsidised mobility services, which require a trustworthy identification within the enrolment phase, and during actual use. In more direct terms, the purpose of this pilot is to adapt an existing German smart mobility app, which allows young adults to use subsidised taxi rides in rural areas. The existing app thus aims to support the mobility of persons in areas where public transportation may not be a viable answer in all cases. In mGov4EU, the objective is firstly to allow the existing app to draw upon the mGov4EU ecosystem to strengthen identification, and more importantly to ensure that it can also be used in a cross-border context, i.e. by non-German young adults. Subsidy mechanisms (i.e. the basic issue of whether a German public authority would want to subsidize the taxi usage of non-Germans) are a political question, and therefore out of scope for mGov4EU.

The interest of the pilot does not lie in its direct added value, since it is uncertain whether there is a significant market demand for cross-border subsidized young adult mobility. Instead, the interest is in determining whether the mGov4EU apps can integrate into existing solutions in order to strengthen security and dependability; and in testing whether the mGov4EU apps can enable pseudonymous but trustworthy attribute attestation. In simpler terms: can the apps allow the verification that a person is indeed a young adult from an eligible country, without divulging more information? That functionality is more broadly applicable and useful than the smart mobility app itself.

From a legal perspective, the main goal of the demonstrator is the enrolment of a new user by directly using a foreign (i.e., non-German) eID, including eIDAS notified eIDs. This would require compliance with the GDPR (for data minimisation and pseudonymity) and the eIDAS Regulation (for derived and trustworthy identity assertions).

2.5.3 e-Signature pilot: international contract signature

The purpose of this use case is to support the creation of advanced electronic signatures, applied to cross-border agreements in a cloud setting, relying on the notified eID means. The Mobile Signature demonstrator seeks to provide a possibility to create advanced electronic signatures in a mobile environment based on a previously performed electronic identification procedure, using electronic

identification means from the different EU Member States that have been notified under the eIDAS Regulation.

The goal is not to create qualified electronic signatures, as would e.g. be envisaged under the eIDAS 2 proposal. Doing so would (among other requirements) involve the use of a qualified electronic signature certificate, issued by a qualified trust service provider, where the signature is created using a qualified signature creation device. These requirements would be too legally and practically cumbersome to manage in a pilot demonstrator. Nonetheless, the demonstrator would in practice demonstrate the viability of trustworthy signing mechanisms, since the goal is to retain the trustworthiness of the original notified electronic identification scheme, and extend this trustworthiness to an e-signature context.

The aim is to demonstrate the applicability of the mGov4EU framework in an international contract signing procedure, involving human signatories and eID means from the different EU Member States and cross-border data exchange processes. The advanced electronic signatures, created in a mobile environment using eIDAS compliant eIDs, will require compliance with the GDPR and the eIDAS Regulation.

Chapter 3 Description and summary of the European legal landscape, and identification of the resulting requirements

In the Chapters above, the principal relevant legal frameworks were identified and described at a high level. This chapter provides more detail on each framework and addresses the relevant requirements for the mGov4EU project.

3.1 Privacy and data protection

3.1.1 General Data Protection Regulation

Both the right to privacy and to the protection of personal data are fundamental rights, enshrined in the EU Charter of Fundamental Rights, respectively in Articles 7 and 8. The right to privacy generally relates to the right to respect for an individual's private and family life, home, and communications. The right to protection of personal data relates to the right of any individual to have data relating to them processed (i.e. collected, stored, exchanged or otherwise used) in a fair and lawful manner. More specifically, the Charter requires that such data is only "*processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified"*. The Charter furthermore requires that compliance with these rules is subject to control by an independent authority.

These generic descriptions are outlined in greater detail specifically in the GDPR, which outlines the principles and requirements for fair and lawful processing of personal data. By now the GDPR should be a well-known piece of legislation, as it has been in force for more than three years now, and tackles issues to which European citizens pay relatively close attention to.

The GDPR applies in principle to any processing (i.e. collection and any other use, including simple exchanges or storage) of personal data, defined as any information relating to an identified or identifiable natural person (a 'data subject') (Article 4 (1) of the GDPR). Since personal data includes any information that can be linked to identified or identifiable persons, and the entire concept of mGov4EU focuses on allowing citizens to manage their data, it is unambiguously clear that the GDPR must be considered in almost any action undertaken in the framework of the mGov4EU project such as piloting, internal project organisation, surveys, data analysis, etc.

Specifically, during the pilots, considering that the end-users are always natural persons, information relating to them will be qualified as personal data, as defined under EU law. The platform thus needs to be designed with privacy and data protection in mind, in accordance with the privacy by design and privacy by default principles of European data protection law.

The GDPR contains the following fundamental principles (Article 5.1 of the GDPR):

- personal data must be processed in a **lawful and transparent manner**, ensuring fairness towards the individuals whose personal data is being processed ('lawfulness, fairness and transparency');
- there must be **specific purposes** for processing the data and the company/organisation must indicate those purposes to individuals when collecting their personal data. A company/organisation can't simply collect personal data for undefined purposes ('purpose limitation');
- the company/organisation must collect and process **only the personal data that is necessary to fulfil that purpose** ('data minimisation');
- the company/organisation must ensure the personal data is accurate and up-to-date, having regard to the purposes for which it is processed, and correct it if not ('accuracy');

- the company /organisation can't further use the personal data for other purposes that aren't **compatible** with the original purpose;
- the company/organisation must ensure that personal data is **stored for no longer than necessary** for the purposes for which it was collected ('storage limitation');
- the company/organisation must install appropriate **technical and organisational safeguards** that ensure the security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technology ('integrity and confidentiality').

Other principles include the obligation to implement **data protection by design** and **data protection by default** in any new initiatives (Article 25 of the GDPR, sometimes also referred to as privacy by design and privacy by default), implying respectively that data protection compliance must be built into architectural designs at the earliest possible stage, and that any features that protect personal data must be activated by default.

As a final principle, the GDPR adopts the **accountability principle** (Article 5.2 of the GDPR**,** meaning that the organisation determining the means and purposes of data processing (the so-called data controller) is responsible for, and be able to demonstrate compliance with, its compliance obligations. In practical terms, that means that the controller must not only assess its compliance but also that it must retain sufficient documentary evidence in order to prove its compliance at all times. Accountability can be supported through systematic and formalised risk assessments, notably through data protection impact assessments (DPIAs), which are strongly recommended upon finalisation of the pilot definitions.

Beyond these principles, the GDPR contains numerous operational and procedural safeguards, including the supervision of data processing activities by an independent authority (a data protection authority, Article 51 and following), a **limitation on transfers of personal data to countries outside the European Economic Area** (EEA) (Article 44 and following), safeguards against the processing of special categories of personal data (such as data concerning health; Article 9) and against automated individual decision-making, including profiling (Article 22 of the GDPR), and rules and procedures on how to deal with incidents involving personal data (so-called personal data breaches, Article 33 and following). Data subjects should also be able to exercise specific predefined rights, such as the right to access copies of their personal data, to halt or limit data processing, and to have their data deleted by the current holder and by any parties to whom they have provided copies of the data (the so-called right to be forgotten). To enable the effective exercise of such rights, infrastructure such as mGov4EU can be eminently suitable.

The GDPR comprises the general legal framework for personal data processing in the EU. Similar and comparable legislation exists for the processing of personal data by EU institutions or in the context of law enforcement, but since these are not in the scope of mGov4EU, they will not be examined in any detail here.

Another legal source that warrants inclusion in this report is the e-Privacy Directive, as amended in 2008. This Directive governs the provision of electronic communication services, in particular management of customer data and definition of specific customer rights (separate from and in addition to GDPR rights). The Directive typically applies to traditional telecoms companies and internet service providers. Nonetheless, it is also relevant to mGov4EU, since the Directive also governs the use of cookies and other tracking technologies that require storage and use of information on the user's device. Generally, such tracking is highly regulated, and only possible with the user's consent, having been provided with clear and comprehensive information about the purposes of the tracking. For completeness, it can be noted that the e-Privacy Directive has been under revision for some time, in order to align it better to the approach of the GDPR, and to ensure that the Directive also covers online services (so-called information society services). While the proposed e-Privacy Regulation has not yet been adopted, it is prudent to observe the rules of this framework, in terms of safeguarding communications confidentiality, abstaining from the use of tracking technologies without consent, and not capturing location data without user consent.

3.1.2 Allocating responsibilities in the mGov4EU constellation

A key question when determining data protection obligations is the allocation of the roles defined under the GDPR. Since the mGov4EU architecture is decentralised and has no central storage of personal data, this is relatively simple:

- First, at the end-user level (i.e., the citizen having the mGov4EU app on their mobile device). Users are the data subjects, i.e. the natural persons for whom the personal data is processed. They must be duly informed of the processing of their personal data, and a legal basis must exist for any data processing on or via their device. Since there is direct interaction with the users in all mGov4EU use cases, their legal consent is the principal and most easily viable option. This means the appropriate information policies must be prepared, and implemented through a layered approach, i.e., the system should support notification to the user at appropriate times. The citizen is not a data controller independently, since their use of the mGov4EU app generally falls under the exemption of personal and household data processing as defined in the GDPR. Thus, citizens have significant rights, but no direct obligations under the GDPR, as long as their use is limited to non-professional purposes. Given the pilot descriptions, in mGov4EU this is not a challenging requirement.
- There is no central mGov4EU platform/system operator that bears separate responsibility as a data controller. While the consortium as a whole should ensure that privacy by design and by default are fully supported, specifically by adhering to the principles below, the consortium (or its members) as such does not bear responsibilities as controllers (or processors) merely by virtue of creating the ecosystem. This assessment changes however when they are involved in pilots, since this is where the purpose of data use is defined, as described in the next bullet point.
- However, mGov4EU generally implies that personal data can be transferred onto a mobile device from a data holder, or that it can be moved from a mobile device to a data consumer. The data holder and data consumer have their own purposes in mind when participating in such exchanges, and will generally be qualified as independent data controllers. This implies that they need to adhere to the principles of the GDPR, including by not processing more data than they need, defining and communicating the purposes for which the data will be used, ensuring transparency, and verifying that they have a legal basis for processing the data.

3.1.3 List of data protection and privacy related requirements

On the basis of the analysis above, a series of data protection and privacy related requirements can be identified (see **Fehler! Verweisquelle konnte nicht gefunden werden.**):

Table 2: Table on data protection and privacy related requirements

Identifier	Description
DP-01	Any citizens are free to choose to use the mGov4EU services, on the basis of their **consent,** which must satisfy the requirements of the GDPR. This implies that alternatives to the mGov4EU services must be available, and that the system must support the withdrawal of users' consent at any given time, which must result in their data being removed from the platform. However, this legal basis doesn't necessarily apply to the service providers use of any received information.
DP-02	Data consumers of the mGov4EU services **may not process the data for other purposes** than those to which the citizen consented. This includes a prohibition on tracking, profiling, data selling or trading, surveillance, or direct marketing – except where a user consented to this.

Identifier	Description
DP-03	Given the consent requirement, the mGov4EU system **may not be used by minors under 16 without parental consent,** nor by any other persons who are not capable of providing legally binding consent.
DP-04	mGov4EU must implement policies and interfaces towards the service providers that **specify what service providers are allowed to do, and what they are not allowed to do.** This includes clear communication of the purposes of use, and a legal commitment to respect this constraint; and implementation of the data minimisation principle – no service provider may request more data than they strictly need.
DP-05	mGov4EU must foresee **transparency notices** that inform citizens of their rights and of the key features of the mGov4EU system.
DP-06	mGov4EU must foresee features that ensure that **no personal data is shared with third parties without user consent.**
DP-07	mGov4EU must foresee **transparency interfaces towards the citizens** that allow them to view and manage data storage, availability and use, including at a service provider-specific level, and that allow them to monitor present and past use of the platform (including any prior authorised data exchanges).
DP-08	mGov4EU must foresee **data subject rights interfaces**, allowing citizens to see, update and delete their personal data on the mGov4EU system; and that allow them to obtain copies of that data (right to access).
DP-09	mGov4EU must implement **storage limitation policies –** by default, data should be deleted from the app after a pre-set period of time, which the citizen may set or modify. Note that this deletion principle does not affect retention duties that can apply to the data controllers themselves – the mGov4EU project cannot override statutory retention obligations; it can only enforce good practices on the apps themselves.
DP-10	mGov4EU must implement the **data protection by default principle,** meaning that any data protection features must be enabled (not disabled) by default. This includes data deletion by default after a set period of time, and no sharing or monetisation of data by default (without user consent).
DP-11	mGov4EU must implement appropriate technical and organisational **security** features. At a minimum, this entails: • Access controls: data on the platform may not be accessible to third parties without citizen consent. Data must be effectively encrypted, and/or it may be protected by other suitable access controls (such as multifactor authentication). • Transfer controls: any personal data sent from the mGov4EU infrastructure to a service provider must be protected against unlawful interception through effective encryption. • Logging and audit trails: exchanges of information to and from the mGov4EU infrastructure must be logged in a way that allows interactions to be identified and examined.
DP-12	Prior to piloting, a **data protection impact assessment** should be conducted on the general mGov4EU architecture and for the use cases, given the innovative use of new technologies that can conceptually pose risks to the rights and interests of the citizens.

Identifier	Description
DP-13	Any service providers with whom the citizen chooses to interact must be **clearly and unambiguously identified to the citizen,** including a description of their role and responsibility.
DP-14	When sharing personal data between consortium partners (e.g. in the context of piloting), the relevant partners must sign a **Data Processing Agreement (DPA)** tailored to the context. As a minimum, the DPA should specify the categories of data subjects and personal data that they will process, the nature of the processing, the purposes of processing, and any (sub)processors involved in the processing of personal data.

No requirements in relation to third-country transfer controls are foreseen. Under such controls, the citizen must be able to see whether data will be sent to a recipient outside of the EEA prior to consenting to sending that data. However, since this does not apply to mGov4EU piloting activities, the requirement will not be implemented.

3.2 Identification and authentication

The verification of the identity of the users is a transversal requirement for trustworthy electronic transactions, and so is the determination by the parties involved of the integrity and authenticity of the exchanged information. This however does not mean that fully anonymous transactions (where it is entirely impossible to identify a citizen, even with the cooperation of other parties such as law enforcement bodies) are not valuable for the European information society. Indeed, they are arguably critical for a democratic society. However, in order for transactions to be trustworthy for relying parties, it will typically be necessary for them to be verifiable.

Similarly, pseudonymous transactions, where a user is not directly identifiable for a relying party, but where the accuracy of the pseudonymous statements can be verified, are on the other hand very important for an advanced information exchange architecture such as mGov4EU.

The faculty to make minimal statements in relation to a user without necessarily divulging their identity (“This person is a minor”; “This person resides in this area”; “This person is a student”) are a key feature of any PIMS. In those cases, the relying party cannot learn the identity of the claimant but knows that the identity of the claimant is known by a third party that vouches for the accuracy of that statement.

As noted above, this issue is regulated by the eIDAS Regulation, which addresses three principal topics (electronic identification, trust services, and electronic documents), and is presently undergoing revision. A proposal for an update to the eIDAS Regulation (sometimes referred to as the eIDAS 2 Proposal, or European Digital Identity Regulation) was published in June 2021.

The proposed new regulation notably improves support for mobile-based approaches, including remote signing solutions. It also creates a legal recognition of electronic attestations of attributes (for which no specific legal basis existed yet), and provides both a definition, a non-discrimination principle, and a legal recognition of electronic ledgers (defined as “a tamper proof electronic record of data, providing authenticity and integrity of the data it contains, accuracy of their date and time, and of their chronological ordering”).

Another new element particularly relevant for mGov4EU is that the proposed regulation would require the EU Member States to offer a European Digital Identity Wallet to their citizens. Such a Wallet, similarly to what is envisaged in the mGov4EU project, would allow users to store identity data, credentials and attributes linked to their identity, and to:

- provide them to relevant parties on request and to use them for authentication, online and offline, in online services; and

- sign via qualified electronic signatures.

Under the proposal, a European Digital Identity Wallet (EDIW) must:

- Be issued by an EU Member State, or under its mandate, or be recognised by an EU Member State (comparable to the approach for eIDAS identity schemes, which must similarly be controlled in some form by the Member States). The EDIW must be able to identify the user at a degree of assurance that is equivalent to the 'high' level of assurance under the existing eIDAS Regulation – meaning in practice that it meets the highest defined standards of assurance – and should be usable for nearly all common e-government applications in the EU.
- Enable user to securely request and obtain, store, select, combine and share, transparently and in a traceable manner identification data and electronic attestation of attributes to authenticate online and offline to use online services, as well as sign by means of qualified electronic signature. In this context, an electronic attestation of attributes is defined as "an attestation in electronic form that allows the authentication of a feature, characteristic or quality of a natural or legal person or of an entity, in electronic form", i.e., an attribute;

Furthermore, the EDIW must be able to act as a common interface for qualified and non-qualified service providers, and for relying parties (i.e. service providers in the context of mGov4EU) requesting and validating person identification data and electronic attestation attributes. Finally, the user shall be in full control of their EDIW.

The proposal also envisages the technical standardisation of Wallets across the EU. In that way, the Wallets potentially could become the principal access keys to public and private services in the EU.

For the purposes of mGov4EU, it is also significant that the Wallets represent an unambiguous shift towards greater individual data sovereignty, since they do not merely comprise a tool for basic identification and signing functionalities, but also act as a secure repository of trustworthy data under the user's control. In effect, the Wallets are a component of the vision that mGov4EU aims to realise.

The eIDAS Regulation (and its potential future evolution with the June 2021 proposal) thus creates a flexible and powerful legal toolset for identification and validation at the cross-border level.

For that reason, the Regulation (but not yet the mobile-oriented revision proposal) is also directly referenced and mandated by the SDGR and its draft Implementing Act, which requires once-only exchanges to use and recognise eIDAS nodes.

On the basis of the analysis above, a series of identification and authentication related requirements can be identified (see **Fehler! Verweisquelle konnte nicht gefunden werden.**):

Table 3: Table on identification and authentication related requirements

Identifier	Description
IA-01	The mGov4EU architecture must be capable of **supporting eIDAS notified identification.** This implies both that it must be possible to create an mGov4EU identity using an eIDAS notified eID, and that service providers should be able to determine who the user is and whether they asserted their identity using an eIDAS notified eID, along with the level of assurance of that eID under the eIDAS Regulation. Note that this **doesn't imply that eIDAS notified eIDs must always or exclusively be used in mGov4EU.** It is perfectly acceptable for non-eIDAS eIDs to be used. However, eIDAS notified eIDs must *also* be usable and recognisable as such, to allow usability of mGov4EU for SDGR purposes.
IA-02	The mGov4EU architecture must be **capable of supporting electronic attestations of attributes** (attribute-based credentials), including through **pseudonymous assertions.**

Identifier	Description
IA-03	Whenever **pseudonymous** transactions are done (including through pseudonymous electronic attestations of attributes), it should be possible to link these to an identifiable citizen with the assistance of third parties (i.e., fully anonymous assertions which are by definition entirely unverifiable should not be supported).
IA-04	The mGov4EU architecture must be capable of **supporting qualified trust services, including qualified signatures and qualified seals.** This only entails that, when the mGov4EU system contains electronic information which is electronically sealed or signed at the qualified level, the architecture does not in any way change, modify, remove or corrupt these seals or signatures. Re-signing or re-sealing is therefore only permissible if the original signatures and seals remain intact and verifiable to relying parties.
IA-05	The **liability and responsibility** of mGov4EU system operators must be clearly and explicitly communicated to service providers interacting with the platform, including notably any exclusions in terms of monitoring, intervention, and quality/integrity/authenticity assurance.

3.3 E-government and public services

The Single Digital Gateway (SDG) was conceived as a platform that creates a bridge between the Member States, and that "*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 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. The single digital gateway will guide citizens and companies to information on national and EU rules, rights and procedures and the websites where they can carry out these procedures online. And users looking for assistance will be guided towards problem-solving services*"[1].

The SDGR creates a legal basis for the creation of the gateway. More importantly from the perspective of the mGov4EU project, it also creates a legal basis for the cross-border exchange of digital evidence between competent authorities in a range of public services. In that way, the objective of the SDGR is to enable the implementation of the once-only principle in European e-government procedures: rather than requiring the citizen to search for their own documentary evidence and requiring them to transfer these from one administration to another, the goal is for reliable evidence to be transferred directly between the relevant public administrations. This increases efficiency, decreases the possibilities for fraud and mistakes, and enhances user-friendliness.

In order to achieve this goal, Article 14 of the SDGR contains the main rules and principles for the cross-border automated exchange of evidence and application of the 'once-only' principle. These can be briefly summarised as follows:

- In terms of **covered services,** the SDGR only applies to a closed list of services. These include online procedures in the context of public procurements (Directive 2014/24/EU and 2014/25/EU), recognition of professional qualifications (Directive 2005/36/EC), access to markets under the Services Directive (Directive 2006/123/EC), and most importantly a long list of online procedures listed in Annex II to the Regulation, addressing a series of so-called 'life events'.

[1] See https://ec.europa.eu/growth/single-market/single-digital-gateway_en

- In terms of **covered entities**, the SDGR applies to "competent authorities". These are defined in the SDGR as "any Member State authority or body established at national, regional or local level with specific responsibilities relating to the information, procedures, assistance and problem-solving services covered by this Regulation" (Article 3 (4) of the SDGR). The notion can therefore also include private entities, but only on the condition that they've been given specific responsibilities in an administrative procedure. Purely private sector transactions (e.g. opening a bank account, or applying for a job directly with a private company) are out of the scope of the SDGR.
- In terms of **covered information,** the SDGR means to facilitate exchanges of 'evidence', defined generically as "any document or data, including text or sound, visual or audiovisual recording, irrespective of the medium used, required by a competent authority to prove facts or compliance with procedural requirements" under the SDGR (Article 3 (5) of the Regulation). In the context of Article 14, the evidence must of course be electronic (since direct online exchanges are required), but there is otherwise no constraint. Evidence may therefore be in any data format, and the evidence can be both structured (e.g. XML documents) or unstructured (e.g. visual PDF scans of original paper documents).
- In terms of **architectural choices,** the SDGR requires exchanges of evidence between competent authorities under the once-only principle to take place via a so-called 'technical system', to be established by the Commission in cooperation with the Member States. The logical components are to be set out in an Implementing Act, which however has not yet been adopted.
- In terms of **procedural safeguards,** the SDGR principally requires that (Article 14):
    - Use of the technical system is **voluntary.** I.e. citizens must always have an alternative available to them, which can be either electronic or paper-based.
    - Evidence may only be exchanged through the technical system based on the **prior request** of the user, i.e. the user must ask for evidence to be exchanged between competent authorities. It is thus not possible for authorities to exchange information without the user's consent, even if this would be in the public interest. Exceptions can exist where there is specific legislation that allows exchanges without any prior request.
    - Evidence may only be exchanged through the technical system after the user has been able to **preview** the evidence, i.e. the user must be able to see evidence before it is sent to a competent authority, and can then decide whether they wish to proceed or not. In that way, the user can verify the accuracy of the evidence, and can also determine whether exchanging it is in their best interest.
    - Exchanges must of course be **secure and interoperable,** to allow trustworthy use of the evidence.
    - Exchanges must be **limited to what is strictly necessary** to what has been requested, and may only be used by the receiving authority for the purpose of the procedure for which the evidence was exchanged.

The SDGR is not directly applicable to the concept underpinning the mGov4EU solution, which enables access to e-government services via a mobile device, but is not limited to it. Moreover, as may have been apparent, most of the pilot use cases do not directly fall within the scope of the SDGR. Nonetheless, the SDGR is relevant as a background consideration for mGov4EU, as the objective is that mGov4EU should also be usable in SDGR related contexts. For that reason, relevant requirements must still be derived, not to ensure that the mGov4EU architecture complies perfectly with the 'technical system' of the SDGR (that would not be possible, since the technical system is controlled by the European Commission and the Member States collectively), but rather to ensure that mGov4EU can be easily integrated with the SGDR.

On the basis of the analysis above, a series of e-government and public services related requirements can be identified (see **Fehler! Verweisquelle konnte nicht gefunden werden.**):

Table 4: Table on e-government and public services related requirements

Identifier	Description
SDG-01	Users must always have an **alternative** to using the mGov4EU infrastructure. The alternative may be electronic, analogue, or physical, but the alternative may not be made unnecessarily difficult or inaccessible.
SDG-02	Recipients of information from the mGov4EU app must always be able to determine the **identity of the entity that issued it**. This may be a private entity, public authority, or the user itself; and the identity may be a pseudonym (including a semantically meaningless number); but the identity must always be assessable to recipients.
SDG-03	No information exchange relating to the user may occur from the mGov4EU app without the **prior request** from the user (i.e., any exchange must be done on the initiative of the user).
SDG-04	Prior to exchanging any information relating to the user from or via the app, the user must be **given the opportunity to view the information, and to decide whether to proceed or cancel.** It is not mandatory that the user actually previews the information; it must only be possible for them to do so.
SDG-05	If the user decides not to exchange any information via the mGov4EU system after previewing it, **then this may not be visible to the relying party.** The relying party should only be able to detect whether an exchange was successful or not, but not whether the failure occurred before or after a preview. Otherwise, the mGov4EU system inadvertently creates a profiling option, since users who decide to cancel an exchange after previewing the information may be considered as suspicious profiles.
SDG-06	Information exchanges must be **granular.** I.e., the user must be informed of the information that the service provider wants, and when multiple sets of information have to be provided to relying parties, the user should be able to select which sets of information (if any) it would like to exchange; the decision should not be 'all or nothing'.
SDG-07	mGov4EU must be conceptually capable of supporting log-on through **eIDAS nodes**. As above, this doesn't imply that eIDAS nodes must always or exclusively be used in mGov4EU. However, eIDAS nodes must also be usable, to allow usability of mGov4EU for SDGR purposes.

3.4 Governance and sovereignty

Both the GDPR and SDGR, as well as the proposed European Digital Identity regulation to a smaller extent, contain elements to support the sovereignty of the citizens over their personal information.

Furthermore, the Data Governance Act, as proposed by the European Commission in November 2020, regulates data sharing services and may eventually set additional requirements relevant to governance sovereignty over data in relation to PIMS.

On the basis of the analysis above, a series of governance and sovereignty related requirements can be identified (see Table 5)

Table 5: Table on governance and sovereignty related requirements

Identifier	Description
GS-01	The mGov4EU platform must have clear **decision-making mechanisms** in relation to architecture, standardisation, scoping and data usage rules. These can be kept lightweight given mGov4EU' status as a research project, but they must be transparent to the citizens, and should never be able to deviate from the primacy of citizen consent.
GS-02	The mGov4EU architecture should **create and promote privacy-preserving data access** mechanisms**.** While using them should not be mandatory, service providers, in particular, should be incentivised to assess whether more privacy-preserving data access (notably based on smaller or pseudonymous data sets) wouldn't also meet their needs.
GS-03	The mGov4EU app should contain a **complaints/rights request mechanism** so that citizens can direct specific problems to the mGov4EU project itself. This does not mitigate or diminish the legal responsibility and liability of service providers but should provide practical assistance to citizens who may struggle to identify responsible parties themselves.

Chapter 4 Piloting requirements

Beyond the generic requirements described above, this section below will briefly highlight some specific challenges and requirements related to the individual pilots. The description below is only a summary at this stage, given that the pilot definitions are still subject to further refinement until M18, and pilot sites (and thus national laws) are still to be determined.

Nonetheless, the descriptions aim to refine the problem analysis above and specify additional requirements.

4.1 I-voting pilot

The pilot as such is not particularly controversial or complex in terms of data protection, considering that the platform already exists and has been publicly audited, and that it can be reasonably assumed to be fully GDPR-compliant already. Notwithstanding, the legal requirements in relation to data protection and identification in the mock election are of course relevant since it is necessary to ascertain that all votes have been cast by eligible voters and that each person votes only once.

The SDGR is not directly applicable, since voting is not a procedure falling within the scope of the SDGR.

Several points of particular attention can be identified.

4.1.1 Privacy and data protection

Data minimisation is a particularly important principle, since the secure processing of voter's personal data in voting may require pseudonymity (or exceptionally true anonymity; but in the case of anonymity, data protection law no longer applies).

Additionally, personal data to be processed should be as minimal as possible. The source information relating to the user for the functioning of the I-Voting system in general requires:

- Either general identification data (for identity verification)
- Or status as a student (to determine eligibility)
- Identifier as a voter and corresponding status (to determine registration: already voted or not)
- Encrypted vote (to determine the actual vote on the chosen topic)

Separately, the I-Voting system will also process personal data about election administrators, and in some cases candidates and auditors (depending on the voting case, i.e. what is being voted on).

More importantly however, data minimisation also requires that this data can be filtered, since it is not always necessary (and often explicitly forbidden) for the party organising the vote to access voting records. In other words, a mechanism must be available that enables pseudonymisation, where the vote organiser receives the encrypted vote and any included pseudonymous data, but no other data. If voting records must be verified (e.g. to determine whether all eligible persons have voted, or to examine claimed voter fraud), this should require support from an intermediary.

Therefore, roles should be allocated as follows:

- University organises the consultation, and acts as a data controller. The University appoints the members of the Election Administration who will securely store the shares of the election private key that needed to decrypt the votes. Thus, they will be the only ones able to jointly anonymise (e.g., using a mix-net) and decrypt the anonymised votes to reveal their contents and tally the results.
- An I-Voting service provider registers all encrypted votes, which are also digitally signed using a pseudonymous identifier for each voter. The online voting service provider and the mGov4EU authentication provider both act as a data processor to the university. They should not collude to ensure that the encrypted digitally signed votes remain truly pseudonymous.

An appropriate data processing agreement must be concluded between the controller and the processors. Additional sub-processors may be involved if the controller agrees.
- The mGov4EU infrastructure (i.e. the app) can retain a locally stored record of the vote on the user's device, if desired.

4.1.2 Identification and authentication

Beyond the issues identified in the description of the EU legal framework, there are no additional challenges. The pilot should support pseudonymity, but this is explicitly permitted under the eIDAS Regulation, including if votes are to be explicitly signed on the mobile device by the user. This would enable pseudonymous assertions to be issued, as is also supported by the eIDAS 2 proposal.

4.2 Smart mobility pilot

Given that the purpose of the Smart Mobility use-case adapts an existing smart mobility solution to support foreign EU MS eID schemes supporting mobile identification, the main requirements are compliance with GDPR and eIDAS requirements.

4.2.1 Privacy and data protection

The pilot as such is not particularly controversial or complex in terms of data protection, considering also that the application already exists, and that (in principle) it should be GDPR compliant already. Moreover, unlike the I-Voting pilot, its existing implementation has no support for pseudonymity.

Nonetheless, the opportunity is to enhance data protection compliance, firstly by reusing trusted eIDAS identity information (rather than a claims-based approach), and by strengthening identity protection through extensive data minimisation (i.e. not providing more information than the claim for subsidized transportation requires).

Persona data required for the functioning of the pilot in general requires:

- General identification data
- Country of residence
- Localisation of the smart mobility service user at the time of the taxi ride order (current location and destination).

During pilot set-up, it will be assessed to what extent a more minimal and pseudonymous approach is practically feasible. In an ideal scenario, mGov4EU can confirm eligibility for the subsidy scheme, by only providing a Yes/No statement to the mobility app ("person qualifies", "person does not qualify"), by assessing only age and whether the person is a resident of an EU Member State. In principle, this information should be sufficient. In practice, more detailed information will be required to schedule rides and to handle payment; but it would be interesting to assess whether compliance can be implemented through a more rigid data minimisation and pseudonymisation approach.

In terms of roles and responsibilities, the relevant stakeholders are:

- The local authority sponsoring the taxi ride. The authority should ideally receive *no* personal data and only pseudonymous statements that an eligible person used a ride.
- The taxi service provider, who should receive the same pseudonymous statement, and information in relation to the ride (and likely payment data).
- The mGov4EU infrastructure (i.e. the app) can retain a locally stored record of the ordered taxi ride on the user's device if desired.

4.2.2 Identification and authentication

The app itself should pose no particular challenges in terms of identification and authentication. In principle, there is no need to use eIDAS notified eIDs or to use qualified signatures as defined by the eIDAS Regulation.

However, while this is not legally required, the use of eIDAS identities and eIDAS nodes will still be tested, in order to determine whether this can increase the reliability of user management for the app without impairing user-friendliness or pseudonymity to a significant extent.

4.3 e-Signature pilot

4.3.1 Privacy and data protection

The pilot as such is not particularly complex in terms of data protection. Electronic signing is a fully decentralised process so that there is minimal data processing involved. In practical terms, electronic signatures should enable linking to a specific signatory (pseudonymously if required) in order to ensure the authenticity of the signature. Signing cannot be perfectly anonymous, for that reason, and the signature data should contain sufficient personal data, likely stored in the signing certificate.

The signature data (i.e. the certificate in a PKI-based model) should thus contain a unique identifier and may contain other identity data insofar as this is proportionate to test functionalities.

In terms of roles and responsibilities, the pilot is similarly not particularly complex:

- The user itself governs its own data on its app, including creating signatures;
- Recipients of signed documents may use the personal data in the signature itself to validate the signature and to otherwise lawfully manage the signed documents, acting as independent data controllers.

4.3.2 Identification and authentication

The e-signature pilot requires a clear link to the eIDAS Regulation, and ideally also to the eIDAS 2 proposal. For that reason, the pilot must either be capable of creating qualified signatures (as is envisaged by the eIDAS 2 proposal in relation to European Digital Identity Wallets), or of creating advanced electronic signatures for which the signature certificates are derived from eIDAS notified eIDs and/or from qualified signature certificates. Either one of these options would allow reasonable assurance for a relying party that the identity information comprised in the signature certificate is trustworthy and legally meaningful in a European context.

Realistically, the second option (advanced electronic signatures derived from eIDs or qualified certificates) is more likely. While this does not result in a qualified signature, there is no transversal European requirement that contracts must be signed using a qualified signature, so that such a pilot is not only useful as a proof of concept, but also for many real-life applications.

Chapter 5 Summary of the impacts on the mGov4EU architecture

5.1 Architectural implications of the legal requirements, and the influence of the SDGR specifically

In the sections above, the principal legal requirements for the mGov4EU project were identified, looking specifically at the influence of the GDPR, SDGR, eIDAS Regulation, and DGA. When examining how these legal frameworks impact the general mGov4EU architecture, it is firstly worth recalling that the SDGR (unlike the other legal frameworks) has a specific architectural model in mind, which is hard coded into the legislation. For that reason, the main architectural constraints emerging from the SDGR should be called out in particular.

As was described in more detail in section 3.3, the SDGR envisages the implementation of a so-called 'technical system', with components at the central (EU) level, and at the Member State level. At a minimum, these entail the following legally required components and functionalities:

- A functional component enabling a **preview of information** to be exchanged is required. The SDGR is mute on whether the component should be centralised or decentralised; and there is no reason why the preview functionality could not be a part of the SDG app to be developed in mGov4EU. Functionally, this component and its interfaces must ensure that information to be exchanged via mGov4EU can be previewed by the user before it is provided to any third party.
- A functional component ensuring that no information occurs without the **prior request** of the user is required. In simpler terms: the SDG app may allow service providers to send information requests to the user, but the app cannot respond to these requests with specific information until the user has provided an authenticated request to do so.
- A functionality allowing the **issuers and recipients of exchanged information to be identified**. The SDGR aims to enable information exchanges between competent public authorities. In mGov4EU, this is done via an intermediation pattern, where the end user receives the information from an issuing authority in the end user's app, and then sends it to the receiving authority via their app. This is permissible, but it must be conceptually possible to determine that the issuer and recipient are indeed competent authorities. To that end, they must be authenticated via the mGov4EU infrastructure.
- A functional component allowing users to **choose which information is made available in any given procedure.** The SDGR requires granular request: it is not sufficient that the user requests or denies information exchanges in a yes/no form; they must be shown which information could be exchanged, and they must be able to select from the available information to determine what they want to exchange, and what they do not. An "all or nothing" approach is not legally acceptable.

These are the main known legal constraints emanating from the SDGR that impact the mGov4EU architecture (as captured also in the more extensive requirements descriptions in Table 4: Table on e-government and public services related requirements. In the sections below, we will provide a broader overview that also examines non-SDGR related requirements.

5.2 Other architectural implications of the legal requirements

The introductory section of this deliverable (specifically section 2.3) described the high level architectural model of mGov4EU. The model showed that the mGov4EU architecture builds on (and extends) the legally mandated SDGR architecture. The mGov4EU app and pilot components in particular are developed specifically for the purpose of the mGov4EU project, and comprise:

- an eID app, which is the local component necessary to activate the eID protocol;

- an eIDAS app to integrate the mGov4EU system with the eIDAS nodes of the EU Member States;
- an eSignature app to support eSignature generation at the initiative of the user;
- and interfaces to SDG components through an SDG app.

These components are also affected by the legal frameworks discussed in Chapter 3. Briefly summarised, the following architectural implications could be deduced from the legal requirements:

- the **eID app must be able to support eIDAS notified eIDs.** While these are not the only legally permissible eIDs under EU law, they are legally required to be usable in SDGR procedures. Therefore, they must be supported in the eID app, which thus must also be connectable to the eID nodes operated under the eIDAS Regulation.
- the **eSignature app must be able to support qualified electronic signatures.** As with the eID requirement, these are not the only legally permissible electronic signatures under EU law; but they do offer the benefit of inherent legal value. Moreover, support for qualified electronic signatures will be required under the anticipated eIDAS 2 amendment. Therefore, they must be supported in the eSignature app.
- The **SDG app must support the secure (unmodified and encrypted) storage of evidentiary documents issued by public authorities.** Since the mGov4EU architecture essentially requires intermediation (with evidence such as diplomas being stored by the user, rather than directly exchanged between public authorities), the mGov4EU architecture must ensure that intermediation does not affect confidentiality or legal validity of information retained by the user.
- In terms of data protection requirements imposed by the GDPR (and thus not linked to the SDGR or eIDAS Regulation):
    - Information storage in the app must be **time limited by default.** No information should be stored without the user's knowledge, and an expiration time should be set by default, after which the information is automatically deleted. The user may choose to override this setting, but this should be an active choice by the user, not a default setting.
    - The **eID app must support attributed based credentials.** Part of the added value of mGov4EU is that not every exchange results in comprehensive and direct identification of the end user. If proof of e.g. age, nationality or eligibility to vote is sufficient, then only this information should be provided (and not also e.g. name, address etc by default).
    - The **SDG app must support transparency notices and data subject rights interfaces.** The user should be able to assess easily who is authorised to use their data and for which purposes, and to exercise their rights (access, correction, deletion, blocking further processing) via the SDG app.

Further legal requirements may emerge when the anticipated Implementing Act under the SGDR is definitively approved, since this may e.g. further regulate where and how the prior request and preview requirement must be implemented, or how overview are kept of competent national authorities who are allowed to access the SDG app. Moreover, the finalisation of the anticipated eIDAS amendment will provide more clarity on the regulatory requirements for European Digital Identity Wallets, to which the mGov4EU architecture aims to align (e.g. in relation to minimal functionalities, or legal frameworks for electronic attribute attestations).

At the time of submission however, these are not yet finalised or available. None the less, it is anticipated that the summary requirements list above should be sufficient to satisfy most or all of the newly emerging requirements.

Chapter 6 Summary and Conclusion

This deliverable aims to provide an initial description of the legal landscape in relation to the mGov4EU project in general, and in relation to the pilots in particular. As the deliverable shows, the legal framework in Europe is already fairly advanced and mature and is suitable for mGov4EU's purposes.

Several challenges will need to be addressed, though. As described in more detail above, the legal framework is not entirely complete or stable yet at this time, with legislative changes still expected in the form of an implementing act under the SDGR, the eIDAS 2 proposal in relation to identity wallets, the proposed Data Governance Act, and an anticipated e-Privacy Regulation. These evolutions will need to be monitored carefully, in particular the eIDAS 2 proposal and the SDGR implementing act, since their choices will affect the future use cases of mGov4EU.

Moreover, the deliverable also shows that, while the envisaged pilots are legally feasible, they also require some challenges to be resolved, notably by implementing rigid data minimisation policies (to avoid needless data disclosure) and by ensuring a clear link to the eIDAS Regulation both in terms of identification and signing. These are two major points where mGov4EU can progress the state of the art, and in which there is significant potential to provide new insights into future policy actions.

Finally, it should also be underlined that this deliverable provides an initial overview and analysis, but that follow-up work is needed to accompany the finalisation of piloting ambitions and in order to create practical legal support texts (including privacy policies and conditions of use) for both the app and the use cases in particular. This work will be undertaken as a part of future Work Package 5 efforts in mGov4EU.

Chapter 7 Bibliography

[1] 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

[2] 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

[3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[4] 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

[5] 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

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

[7] 2017 Tallinn e-government declaration; see https://www.mkm.ee/en/objectives-activities/information-society/tallinn-declaration

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

[9] Proposal for a Regulation Of The European Parliament And Of The Council on European data governance (Data Governance Act), see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

[10] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0058-20091219

[11] 2021 TechDispatch #3/2020 - Personal Information Management Systems by the European Data Protection Supervisor, see https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-32020-personal-information