D5.1

Ethics and Gender Management Framework

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 / D5.1 / V1.1
Work package contributing to the deliverable:	WP5
Due date:	February 2021 – M02
Actual submission date:	30th May 2022

Responsible organisation:	TLX
Editor:	Hans Graux, Mahault Piéchaud Boura
Dissemination level:	PU
Revision:	V1.1

Abstract:	This is the first iteration of the Ethics and Gender Management Framework for the mGov4EU project. It identifies general ethics and legal compliance objectives and guidelines to facilitate their implementation.
Keywords:	Ethics, gender, management, requirements, guidelines

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

Editor

Graux, Hans (TLX)

Contributors

Lampoltshammer, Thomas (DUK)

Krimmer, Robert (UTARTU)

Piéchaud Boura, Mahault (TLX)

Graux, Hans (TLX)

Disclaimer

Executive Summary

This deliverable is the first iteration of the Ethics and Gender Management Framework for the mGov4EU project. It identifies general ethics and legal compliance objectives that should be assessed, evaluated, and complied with throughout the project, along with practical guidelines to facilitate their implementation.

The objectives identified in Chapter 2 of this first iteration are organised into three categories: Privacy and data protection, Technical solution development, and Pilot implementation. The first category contains objectives that ensure respect of the fundamental right to data protection (both at the architectural and piloting level), the second focuses on ethics requirements for the general (non-pilot specific) technical design of the project's architecture, and the last defines functional requirements at the pilot (application specific) level. The focus of each of the three chapters is thus different: the first focuses on data aspects; the second on architectural aspects; and the third on functional (non-data) aspects.

The guidelines in Chapter 3 in contrast do not focus on substantive objectives, but on management of ethics issues, again both at the architectural level and piloting level, covering both data and non-data aspects. They aim to ensure that ethics challenges and potential risks are communicated, mapped, evaluated, and mitigated throughout the project.

Compliance with the objectives will be monitored throughout the project through the execution of the action points identified in this report, including via specific deliverables in Work Package 8; and their actual implementation (along with lessons learned) will be evaluated in the second iteration of the Framework.

The following table summarizes the relation of D5.1 to other tasks, work packages, and deliverables:

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

Contributing tasks of this WP:	T5.3
Input from other tasks/WPs:	-
Output to other tasks/WPs:	T5.4, T6.1
Output to other deliverables:	D5.3, D5.8, D6.2

Table of Content

List of Tables

List of Abbreviations

Abbreviation	Meaning
DPO	Data protection Officer
GDPR	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)
SDGR	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
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for

Abbreviation	Meaning
	electronic transactions in the internal market and repealing Directive 1999/93/EC
DPIA	Data Protection Impact Assessment

Chapter 1 Introduction

Work Package 5 on Evaluation, Ethics and Privacy aims (among other objectives) to establish a framework for ethics and gender management, containing project-wide guidelines, procedures, and tools for covering ethics and gender-related issues. It provides the overarching ethics framework, which is thereafter detailed and operationalised through Work Package 8 - Ethics requirements, focusing on concrete GDPR compliance actions, as well as broader ethics concerns. As a first step in creating this framework in Work Package 5, Task 5.3 identifies legal and ethics requirements to be implemented and monitored throughout the "Mobile Cross-Border Government Services for Europe" (mGov4EU-) Action, as a part of this first deliverable D5.1.

As stated in the description of the action, mGov4EU will develop an open ecosystem for secure mobile government services to be used across Europe and beyond. To that end mGov4EU will 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.

This deliverable is the first iteration of the Ethics and Gender Management Framework for the mGov4EU project. It identifies general ethics and legal compliance objectives that should be assessed, evaluated, and complied with throughout the project, along with practical guidelines to facilitate their implementation.

The framework will be developed, refined, and completed throughout the project. The actions undertaken and the results of their implementation (including lessons learned) will be compiled in the second iteration of this deliverable, due at the end of the project. Therefore, this framework should not be considered a conclusive and static document, but rather an initial identification of relevant requirements for the development of a mobile government ecosystem, along with a statement of the procedures to ensure that these requirements are adhered to, and that ambiguities can be identified and resolved proactively.

The ethical and legal concerns identified at this stage mainly arise from the processing of personal data in the context of piloting activities, and more generally in the design and operation of the mGov4EU architecture. Therefore, the impact of General Data Protection Regulation and the EU Charter of Fundamental Rights (as a source recognising the fundamental right to data protection) must be considered. However, compliance with requirements of the Single Digital Gateway Regulation and the eIDAS Regulation should be considered as well, since both pieces of legislation contain fundamental rules and principles relating to the once-only exchange of administrative evidence, and the identification and authentication of users. Finally, broader (non-data) ethics challenges must be identified and managed as well, driven by the EU's fundamental rights framework.

This deliverable will first identify the substantive ethics and gender compliance objectives, based on a preliminary analysis of the aforementioned sources, and then set up general procedural guidelines to support their implementation in the course of the project.

Chapter 2 Ethics and gender management principles

The general purpose of this document is to develop an ethics and gender compliance framework for the development of the mGov4EU solution. In order to do so, it is important to state explicitly what the substantive requirements to be complied with are.

Therefore, in this section we identify the main ethical and gender management objectives to be considered throughout the mGov4EU Action.

For each of these objectives, high level requirements are identified, as well as specific action points for mGov4EU. In the course of the mGov4EU Action, including the architectural design and the pilot implementation, concrete measures required to achieve the objectives will be documented through specific controls (i.e., the implementation of a Data Management Plan (D6.2), the completion of data protection impact assessments, risk assessments, gathering consents, drafting information notices, etc.). The results of their implementation will be reported in the second iteration of the Ethics and Gender management Framework.

The objectives are organised in three categories: Privacy and data protection, Technical solution development (architectural requirements), and Pilot implementation (including non-data driven ethics challenges).

2.1 Privacy and data protection objectives

Privacy and data protection must be considered at all stages of the life cycle of any service aiming to collect, transfer, or otherwise use personal data. Therefore, all data protection principles, as laid out in the General Data Protection Regulation, must be fully respected during all piloting activities.

The objectives stated herein apply equally to architectural design, piloting activities, and project management.

Fair and lawful processing objectives

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. Open, honest, and understandable communication with the data subject concerning the processing activities must be in place.

As a result, for any data processing activity in the context of mGov4EU, the project should:

- Identify the relevant legal basis for the specific activity, including an assessment of whether consent of the data subjects is feasible and appropriate.
- Prepare appropriate information notices for data subject, and identify a contact point for further information, including any relevant DPO.

Purpose limitation objectives

Personal data may only be collected for specified, explicit and legitimate purposes and may not be further processed in a manner that is incompatible with those purposes.

As a result, for any data processing activity in the context of mGov4EU, the project should:

- Identify and explicitly state the purpose of processing.
- If existing data are reused, carry out a compatibility assessment with the initial purpose of processing, and rectify any legitimacy concerns.

Data quality and storage objectives

The data collected must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. The personal data processed must be accurate and, where necessary, kept up to date.

Therefore, every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay. Personal data is stored in identifying format for no longer than is necessary for the purposes of processing.

As a result, for any data processing activity in the context of mGov4EU, the project should:

- Ensure that the data collected and processed are limited to the minimum necessary to achieve the purposes. This implies avoidance of standardised routine procedures that apply the same data processing techniques to procedures with different requirements. This also implies maximisation of pseudonymisation and anonymisation techniques during all project activities.
- Ensure that the data is only stored for the minimum duration necessary to achieve the purposes. This implies that data retention, deletion and/or anonymisation policies are explicitly stated in all data processing activities.
- Ensure that data is shared with, and retained by, the smallest number of entities possible at all times. Centralised data storage must be avoided when there is no functional necessity for it.
- Define procedures to ensure that the data is correct and up to date, including through proactive error detection during inputs where necessary, and providing the possibility to correct the data.

Security objectives

The personal data must be processed in a manner that ensures appropriate its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

Furthermore, measures that can be used to demonstrate compliance must be taken, such as logs of processing and documentation detailing the processes.

As a result, for any data processing activity in the context of mGov4EU, the project should:

- Implement appropriate technical and organisation measures considering the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity.
- Document security procedures and choices in written policies, including a justification of their suitability given the context of processing activities.

Monitoring objectives

Records should be kept of data processing choices made in the course of the project. It must be possible to determine at all times that data protection law is complied with, including by maintaining an up-to-date overview of data processing activities:

- Establish and maintain records of data processing undertaken specifically in the context of the mGov4EU project.

- Establish and maintain records of any incidents that may occur in relation to personal data in the course of the project, including anticipated impacts, risks, and mitigation measures taken.

2.2 Technical solution development objectives

The objectives identified in this section should be achieved by any non-pilot specific components developed in the course of mGov4EU, and therefore should be considered in the architecture of the system.

The definition of objectives and their execution in the mGov4EU project will be driven to some extent by the SDGR, and its further evolution in the future, notably through the adoption of an Implementing Act by June 2021, outlining specific requirements and details of the technical system that will be used to operationalise the once-only principle. However, high level objectives can still be stated, since the SDGR itself and its objectives are stable, and since the mGov4EU project aims to build on the SDGR realisations rather than being entirely constrained by them. In other words, while mGov4EU outputs must be usable to enhance the functionality and value of the SDGR, mGov4EU can innovate in ways that extend beyond the constraints of the SDGR and its Implementing Act. None the less, to ensure the validity and usability of mGov4EU project outcomes, the project will constantly evaluate the impact of the legal framework for once-only exchanges in the EU, including from a privacy standpoint for a possible impact on the pilots and their design.

Good administration objectives

A solution developed to support mobile government should support the principle of good administration, and therefore should ensure that use cases can be handled impartially, fairly, in compliance with applicable national and European laws and norms and within a reasonable time.

As a result, for any data processing activity in the context of mGov4EU, the project should:

- Ensure that all users will receive equal treatment.
- Ensure that all users will have access to recourse in case of disputes and incidents.
- Ensure that there is a legal framework (including any contractual frameworks or policies) for the handling of personal data or other information exchanged between architectural components.

Accountability objectives

A solution developed for mobile government should consider the accountability requirement, thus ensuring the recording, reporting and explainability of decision taken, and ensuring the responsibility of decision makes, as well as providing for effective remedies in the event of a dispute.

As a result, for any data processing activity in the context of mGov4EU, the project should:

- Ensure that the solution support accountability for users and any administrative authorities alike.
- Support accountability for any processes specific to the mGov4EU architecture, including by providing appropriate documentation, contact points, and by defining an organisational structure that is conducive to a clear allocation of responsibilities.
- Identify any risks that could give rise to liabilities specific to the mGov4EU activities, along with any required mitigation measures. This will be done in interaction with WP7 (Project, Risk and Innovation Management), which includes a specific risk management task (T7.2).

Justice objectives

A solution developed for mobile government should ensure the right to be heard and fair treatment for users. Therefore, it should provide a mechanism to register a complaint against a decision resulting from a procedure initiated through the mGov4EU architecture.

As a result, for any data processing activity in the context of mGov4EU, the project should:

- Ensure that the design provides easy mechanisms for the user to contact relevant administrative authorities for questions or complaints.
- Ensure that the design supports the fair and equal treatment of users in a verifiable manner.

Privacy and data protection objectives

A solution developed for mobile government must be mindful of the privacy of its users and take particular care to data protection principles and ensure compliance with the applicable data protection legislation (European and national).

As a result, for any data processing activity in the context of mGov4EU, the project should:

- Ensure that the design is compliant with all principles set out in section 2.1.
- More specifically, the principles of data minimisation, storage limitation and purpose limitation are critical in the context of mobile-enabled once-only procedures. It should be ensured that mobile data storage creates no new vectors for unlawful storage, exchange, or re-use of the data; and that once-only exchanges do not result in needless duplication of data storage.
- Ensure that the design is developed in accordance with the principles of data protection by design and by default as commented in section 3.3.

Security objectives

A solution developed for mobile government must be secure for its users. The exchanged evidence accessible through the solution and the personal data provided by the users must be protected against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the evidence, thereby ensuring its integrity and authenticity.

As a result, for any data processing activity in the context of mGov4EU, the project should:

- Ensure the security of information stored or accessed through any components designed by mGov4EU. These should not be accessible or usable without user control.

2.3 Pilot implementation objectives

All piloting activities in mGov4EU should be compliant with ethical principles and relevant national, Union, and international legislation, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its Supplementary Protocols.

Objectives related to general (non-data) ethical compliance

To achieve these goals, piloting activities should undergo a summary human rights impact assessment, to determine whether they are likely to generate challenges with respect to key fundamental rights protected by the aforementioned Charter, as summarised hereunder:

Table 2: Human rights impact assessment (non-data aspects)

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

Each pilot should, prior to initiating, assess whether a right or freedom is likely to be impacted (positively or negatively), and in case of negative impacts, how these can be avoided or mitigated in an adequate manner.

Objectives related to the selection of pilot participants

The involvement of natural persons in mGov4EU is not related to social science and humanities research, nor do the piloting activities relate to research involving children, persons with diminished capabilities, or sensitive data. Therefore, personal aspects, traits, or characteristics will not be evaluated during piloting.

The personal data of individuals volunteering for mGov4Eu piloting phase will used to test the solutions and to perform demonstrations showcasing how the solutions developed during the project would work in practice.

It follows that the criteria used to select data subjects for the project do not relate to specific physical or personality traits but relate only to parameters relevant to the (administrative) procedures they which complete in the frame of the pilots.

- The procedure for the enrolment of the pilot participants will be established by the consortium partners in charge of the pilots, taking in consideration the specificities of each pilot. The partners concerned will observe the requirements of applicable data protection legislation, including but not limited to the GDPR, when processing such personal data, as well as the applicable national legislation must be given.
- Persons who are unable to provide legally valid consent as required under the GDPR (including minors) will not be involved in piloting activities.

Lawfulness, consent and information objective:

The lawfulness of any data collection and processing in mGov4EU should be ensured at all times. Wherever consent can be obtained in a legally valid manner, the individuals volunteering to participate in mGov4EU pilots will be asked provide their consent in compliance with the requirements of the GDPR. In other words, consent is the favoured legal basis for piloting activities in mGov4EU. To be valid such consent must be freely given, specific, informed, and unambiguous. The consent can be collected verbally, electrically or in written format, and must be recorded.

It is however anticipated that consent will not always be legally possible in all mGov4EU piloting activities. In order to be valid under the GDPR, consent must be freely given, and this is not possible in situations where there is a clear imbalance of power between the data controller (the party asking for the consent) and the data subject (the party giving their consent). Such an imbalance of power is e.g. presumed to exist in an employment context or when students are asked to participate, given that such persons may have concerns about negative repercussions if they deny their consent. Some piloting activities may initially be undertaken with employees of the beneficiaries (internal testing) before going live, or with students. In such cases, an alternative legal basis will be sought before proceeding with piloting.

Separate from the lawfulness issue, the information objective must always be satisfied. To meet the information objective, the pilot volunteer must be aware of the purpose and modalities of the pilots, that they have the possibility to withdraw from pilot participation. Such information must also contain the require information under applicable data protection legislation.

As a result, for any data processing activity in the context of mGov4EU piloting, the project should:

- Define the consent procedures, including recording and withdrawal of consents.
- Evaluate the legal basis (consent where possible, alternatives where needed) before proceeding with piloting
- Draft suitable information notices in accessible language.

Accountability objectives

Accountability of the partners is achieved through an appropriate documentation of processes, covering compliance with relevant European and national legislation, and the systematic

involvement of DPOs to review and approve mechanisms framing the involvement of pilot participants.

As a result, for any data processing activity in the context of mGov4EU piloting, the project should:

- Defined and log categories of data necessary, the purpose of processing, legal base of processing and storage duration for each individual pilot.
- Human rights impact assessment as explained above.
- Identify and assess relevant risks for any piloting activity prior to pilot initiation, as explained in section 3.2 below.
- Ensure that any piloting activity minimises the risks of harm to the users, through the implementation of appropriate technical and organisational measures, and operational controls that ensure that incidents can be identified, mitigated, and resolved.
- All relevant accountability documentation should be submitted to the competent DPO(s) for their opinion.

Gender management objectives

While the piloting activities in mGov4EU are not conceptually expected to affect one gender differently than any other, actions should be undertaken to verify and ensure that this expectation is accurate, and that no gender bias occurs.

As a result, for any data processing activity in the context of mGov4EU piloting, the project should:

- Aim at ensuring reasonable balance in gender representation during piloting activities.
- Evaluate after piloting whether any no gender imbalances have taken place, and whether piloting affects persons of different genders differently.
- Periodically report on gender balance in persons involved in the project, in accordance with Horizon2020 reporting standards

Chapter 3 Ethics management guidelines

The ethics objectives identified above should guide the development of the mGov4EU technical solution as well as its piloting. This section introduces procedural guidelines that must be respected by all project partners to ensure that the aforementioned ethics and gender management principles are complied with.

3.1 Systematic involvement of the legal and ethics partner in the architecture design

The ethical and legal partner must be informed of the architectural choices in a timely manner to support the respect of legal and ethical requirements and identify any compliance issues, and potential mitigation actions. Where no practicable alternative solution can be found, residual risks must be documented and accepted before proceeding.

The architectural development must be mindful of the principle of data protection by design and by default as explained in more detail in section 3.3 below.

Additionally, the architecture design must taken into account the requirements imposed by the SDGR, and its further evolution in the future via the anticipated Implementing Act (due in June 2021). The project will constantly evaluate the impact of the legal framework for once-only exchanges in the EU, including from a privacy standpoint for a possible impact on the pilots and their design.

The architectural choices in terms data requirements should be appropriately reflected in the Data Management Plan, which must provide accurate information on:

- the purpose of the data collection/generation and its relation to the objectives of the solution developed, and by whom it will be used;
- the types and formats of data the system will generate and or collect, and its expected volume (at least at pilot stage);
- the origin of the data;
- whether the system will re-use data, and if so, how.

Any changes in these choices, or other changes in mGov4EU planning that could affect the integrity of the Data Management Plan must be notified to the legal and ethics partner, so that they can be appropriately documented and assessed.

3.2 Involvement of the legal and ethics partner in relation to piloting activities

The ethical and legal partner must be informed prior to the initiation or modification of any piloting activities in a timely manner to identify any potential risks and compliance issues with the legal and ethics requirements.

mGov4EU should cooperate in good faith to carry out a risk assessment of the pilots before launching the activity. The analysis must determine the level of risk of the piloting activities:

- Low risk piloting activities are piloting activities that involve *only* fictitious users, fictitious data, and test procedures (not affecting production environments).
- Medium risk piloting activities include piloting activities that involve any one or two of the following factors:
    - Real users
    - Real-life data
    - Production environments

- High risk piloting activities including piloting activities that involve real users, real-life data, and production environments.

Based on the risk assessment appropriate mitigation measures must be defined and implemented in consultation with the ethical and legal partner, following at least the constraints identified below:

Table 3: Table on pilot risk classification

Level of risk	Constraints
Low risk	- The assessment of risk should be notified and recorded
Medium risk	- The assessment of risk should be notified and recorded - Active communication of the risks and consequences to the pilot participants, and offering the possibility to withdraw at any time - Performance of the pilot under the supervision of the DPO (or if none is available, the mGov4EU legal/ethical partner) - Monitoring to detect and remedy/ mitigate incidents
High risk	- The assessment of risk should be notified and recorded - Active communication of the risks and consequences to the pilot participants, and offering the possible to withdraw at any time - Performance of the pilot under the supervision of the DPO, and with involvement of the mGov4EU legal/ethical partner - Notification duty to the DPO and the mGov4EU legal/ethical partner of any piloting incident that may negatively impact the users - Definition and implementation of a risk monitoring strategy that covers all parts of the piloting activity - Monitoring to detect and remedy/ mitigate incidents

3.3 Implementation of the principles of data protection by design and by default

The development of all mGov4EU components must comply with the principles of data protection by design and by default as defined in article 25 of the GDPR.

The implementation of these principles requires the consideration of data protection at the design stage of a project. This relies on an identification of the data necessary for the purpose of the system and for the pilots, and the potential risks to the fundamental rights and freedoms of the data subjects (i.e., the users).

The implementation of these principles must be continued throughout the lifecycle of the system, i.e., throughout the mGov4EU project's duration. The table below will be available to the partners throughout the projects and must be kept up-to-date.

Table 4: Table on the types of data used

Categories of data	Purpose	Means of collection	Recipient(s)	Storage modality

Table 5 : Table on the risks identified and possible mitigation measures

Risk	Impact	Likelihood	Severity	Mitigation measures
		Choose an item.	Choose an item.	
		Choose an item.	Choose an item.	
		Choose an item.	Choose an item.	

The information gathered through this table will be used as a basis for a Data Protection Impact Assessment for the solution developed through mGov4EU and for its piloting activities.

Chapter 4 Summary and Conclusion

The purpose of this deliverable is to establish the basic components of the Ethics and Gender Management Framework. The identified elements will be monitored throughout the project and the subsequent action points will be reported on in the second iteration of the Framework (D5.3); and operationalisation of these elements will occur through Work Package 8 - Ethics requirements, focusing on concrete GDPR compliance actions.

The second iteration of this deliverable will also reflect on the lessons learned in terms of ethics and data protection implementation during mGov4EU.

Action points:

- Identify the purpose of processing and determine the appropriate legal base, based on the input gathered using Table 4: Table on the types of data used.
- Conduct a human rights impact assessment to identify any positive or negative impacts on human rights or freedoms, using the structure in Table 2: Human rights impact assessment (non-data aspects)
- The data collected and processed must be limited to the minimum necessary to achieve the purposes. The data may only be stored to the minimum duration necessary to achieve the purposes. If the data set are being reused, carry out a compatibility assessment with the initial purpose of processing. These elements must be monitored through the performance of a Data protection Impact Assessment on the development of the mGov4EU technical solution, which should also be supported by documentation of the architectural and technical choices and reasoning concerning personal data.
- The pilot must ensure the data is correct and up to date, and where necessary and possible provide the means to correct the data.
- Implement technical and organisation measures considering the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity, based on the input gathered in Work Package 5: Evaluation, Ethics and Privacy.
- Establish a procedure for the enrolment of the pilot participants, covering consent procedure and possible withdrawal (D8.2)
- Draft information notices for pilot participants

Furthermore, some of the ethics and legal concerns identified, which are particularly relevant for the development of the system itself may be further specified through the assessment of the legal landscape carried out in Task 5.4 Assessing the Legal Landscape and Regulations, including GDPR and eIDAS. Therefore, the associated deliverable should address the following elements:

- Describe and evaluate the legal framework for the handling of personal data and evidence exchanged between the service provider and the SDG technical solution where relevant, including its future evolutions through the Implementing Act of the SDGR.
- The implementation of technical and organisational security measures proportional to the risk.
- Clearly identify liabilities specific to the mobile service.
- The system should comply with applicable data protection legislation and developed considering data protection by design and by default.
- The principles of data minimisation and storage limitation have considerable impact on the solution and should be considered carefully in relation with the OOP.

Chapter 5 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] 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

[4] 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

[5] 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

[6] Kamraro. 'Responsible Research & Innovation'. Text. Horizon 2020 - European Commission, 1 April 2014. https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation