

# GOVTECH4ALL



Deliverable: D7.1

## Procedures on Ethics Requirements

### No.1

Work Package 7

Ethics Requirements

Version: Final



This project has received funding from the European Union's Horizon Europe Framework Programme under grant agreement N° 101057497.

## Deliverable Overview

This document outlines the rationale for developing the ethics procedures, highlighting their crucial role in upholding ethical practices throughout the project's lifecycle as well as after the completion of the project. By adhering to these ethics procedures, prioritise the protection of participants' rights and data privacy, fostering transparency, trustworthiness, and integrity throughout the project's execution.

## Additional Information

**Type:** Ethics

**Dissemination Level:** SEN

**Official Submission Date:** 30<sup>th</sup> of September 2023

6<sup>th</sup> of October 2023



This project has received funding from the European Union's Horizon Europe Framework Programme under grant agreement N° 101057497.

## Document Revision History

Version	Date	Description	Partners
0.1	01/09/2023	ToC	LC
0.2	03/09/2023	Preliminary review	UNEXT
0.3	10/09/2023	First outline of the strategy	UNEXT
0.4	27/09/2023	Final version of the strategy, for review	LC
0.5	02/10/2023	Final review	UNEXT
1	03/10/2023	Ready for submission	LC

## Authors and Reviewers

### Authors

- Alessandro Paciaroni, The Lisbon Council
- Ethics Advisor, UNEXT

### Reviewers

- David Osimo, The Lisbon Council
- Alex Borg, The Lisbon Council

## Statement of Originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.



This project has received funding from the European Union's Horizon Europe Framework Programme under grant agreement N° 101057497.

## Table of Contents

<b>Executive Summary</b> .....	<b>7</b>
<b>1. Introduction</b> .....	<b>8</b>
<b>2. Ethics in European Union projects</b> .....	<b>8</b>
<b>2.1 Responsible Research and Innovation</b> .....	<b>9</b>
<b>3. Ethics Strategy in GOVTECH4ALL</b> .....	<b>9</b>
<b>3.1 Preliminary Ethics Screening</b> .....	<b>10</b>
<b>3.2 Ethics Assessment</b> .....	<b>10</b>
3.2.1 Impact Assessment Architecture.....	10
3.2.2 GOVTECH4ALL Impact Assessment Description .....	11
3.2.3 Impact Assessment Methodology .....	11
<b>3.3 Impact Assessment Requirements</b> .....	<b>12</b>
3.3.1 GDPR framework and DPIA .....	12
3.3.2 The dynamic compliance process.....	19
3.3.3 Other Legal Obligations Impact Assessment .....	21
<b>3.3.4 Online Monitoring Tool</b> .....	<b>21</b>
<b>4. Conclusions</b> .....	<b>23</b>
Annex A - Dataset description template .....	<b>25</b>
Annex B - GAP analysis and DPIA generation tool and template .....	<b>27</b>



## List of Terms and Abbreviations

Abbreviation	Description
DPIA	Data Protection Impact Assessment
Dx.y	Deliverable x.y
EU	European Union
GDPR	General Data Protection Regulation
GA	Grant Agreement
IA	Impact Assessment
Mx.y	Month x.y
RRI	Responsible Research and Innovation
WPx	Work Package x



This project has received funding from the European Union's Horizon Europe Framework Programme under grant agreement N° 101057497.

## List of Figures

Figure 3-1 - DPIA assessment process .....	15
Figure 3-2 – Ethical Compliance assessment process .....	20
Figure 3-3 – Online Monitoring Tool .....	22

## List of Tables

Table 3-1 - DPIA criteria.....	15
--------------------------------	----



## Executive Summary

This document – Deliverable 7.1 - presents the Ethics Strategy, which encompasses a comprehensive framework for the ongoing ethical evaluation of the GOVTECH4ALL project. Aligned with the stipulations of the Specific Grant Agreement, which mandates the continuous integration of ethical considerations, this strategy serves as a guiding beacon for the endeavours of the GOVTECH4ALL consortium in ethics, responsible innovation, and technology utilisation. The document consists of four key sections:

1. an introduction to the intersection of ethics and technology;
2. a detailed exposition of pertinent clauses from the Grant Agreement and related documents along with overarching principles;
3. the core strategy,
4. and conclusive remarks.

The document is complemented by an Annex which provides templates and tools utilised by the consortium.



## 1. Introduction

This deliverable consists of the ethics assessment strategy for the project GOVTECH4ALL. The strategy outlines the overall approach, tools and methods that the project adopts for the continuous ethical assessment of the work conducted by the consortium, in particular of its pilot projects. The strategy provides an overview of the toolbox made available to the consortium and of the principles that will guide the definition of further actions for a continuous ethics assessment. This is to say that the first and foremost principles of the strategic approach adopted are adaptability and continuous improvement. Such an overarching principle is considered necessary to ensure that the endeavours of the consortium effectively consider ethics principles, and the ethics assessment provides added value to the project by harnessing the benefits of technology and data sharing, rather than adhering to a logic of neutral requirements definition and fulfilment.

The deliverable will outline relevant provisions and principles that guide the structuring of the strategy, as well as delineate the strategy itself before providing concluding remarks

## 2. Ethics in European Union projects

This chapter provides an overview of applicable provisions of relevant contractual agreements -i.e., the Specific Grant Agreement – and other principles considered in European Union funded projects -e.g., Responsible Research and Innovation (RRI).

Article 14 of the Specific Grant Agreement states:

“The action must be carried out in line with the highest ethical standards and the applicable EU, international and national law on ethical principles. Specific ethics rules (if any) are set out in Annex 5.”<sup>1</sup>

Additionally, Article 15 of the Specific Grant Agreement recalls applicable regulations regarding data processing and data protection. The grant agreement foresees the appointment of an Ethics Advisor to ensure the highest standard and relevant experience with the specific practices and approaches related to the ethics assessment.<sup>2</sup>

Annex 5 of the Specific Grant Agreement further specifies the commitment of the consortium to abide by the highest ethical standards and other relevant values and principles such as democracy and rule of law.<sup>3</sup>

Although there is centralised coordination of ethics and data protection, there is decentralised responsibility regarding the implementation of suggested measures. This is compliant with the General Data Protection Regulation provisions regarding Data Protection Officers.

---

<sup>1</sup> GOVTECH4ALL Consortium, *Specific Grant Agreement*, (Brussels, 2023).

<sup>2</sup> GOVTECH4ALL Consortium, *Specific Grant Agreement*, (Brussels, 2023).

<sup>3</sup> GOVTECH4ALL Consortium, *Specific Grant Agreement*, (Brussels, 2023).





In other words, the centralised coordination of ethics and data protection assessment is combined with the decentralised - i.e., organisation by organisation - responsibility towards data protection and conduction of assessments.

In accordance with the abovementioned considerations, the Specific Grant Agreement foresees a Work Package (WP) on ethics (WP7) and deliverables consisting of a strategy and preliminary ethics assessments (addressing the questions of the reviewers from the European Commission).

## 2.1 Responsible Research and Innovation

Responsible Research and Innovation (RRI) broadly entails that Research and Innovation (R&I) and societal values are harmonised and intertwined in a cross-fertilising relationship. On a practical level, RRI devises tools and approaches to engage the public in the research process to better align research goals and outcomes with societal needs, challenges, values, and aspirations.<sup>4</sup>

While the Framework Programme Agreement at hand, and the GOVTECH4ALL project, are funded under the Digital Europe Programme, differing from the other European Union-funded programmes because it is not categorised as a research programme; the principle of responsible innovation stands valid and central to the work of the consortium.

In other words, the societal impact of the project, mainly throughout the implementation and delivery of the pilot projects and the solutions thereof, remains a focus of the consortium throughout the duration of the agreement.

This is reflected in the development of the project per se in the form of the Scalability Framework for the selection of pilot projects - Deliverable 3.2 – specifically in the consideration of elements pertinent to societal impact and in the delineation of criteria against which to assess the scalability of pilot projects.<sup>5</sup>

The GOVTECH4ALL consortium is committed to carrying out actions in accordance with the highest ethical standards and legal requirements. For this reason, an External Advisory Board (EAB) has been established to support the thorough considerations of ethics by means of establishing approaches, work plans and criteria for the ethics assessment. This ensures the consideration of ethics, privacy and data protection throughout the duration of the project.

## 3. Ethics Strategy in GOVTECH4ALL

The ethics governance is assigned to the project coordinator in collaboration with the ethics advisor and to the ethics working group.

The project coordinator together with the ethics advisor is responsible for setting the strategy and all the relevant supporting measures and tools for an effective ethics assessment.

---

<sup>4</sup> Responsible Research and Innovation tools <https://rri-tools.eu/>

<sup>5</sup> GOVTECH4ALL Consortium, Validation Framework and Maturity Assessment, Brussels (2023).



The ethics working group is responsible for acting on the strategic guidance provided by the ethics advisor and the coordinator.

The ethics working group consists of a representative of each organisation involved in the pilot projects and/or that has a role in data management within the project. This representative shall be the partner Data Protection Officer or someone appointed by him. Additionally, the ethics advisor and the project coordinator are members of the ethics working group.

The strategy consists of a preliminary ethics screening and a continuous ethics assessment.

### 3.1 Preliminary Ethics Screening

The preliminary ethics screening was submitted as part of D7.2 as a response to the comments received from the reviewers of the European Commission and in compliance with the Specific Grant Agreement.

“The Govtech4all-beta runs an in-depth verification of Ethics Assessment, following comments received in the EU document: Ethics Screening – Ethics Evaluation Summary Report.

Each point has been addressed, although the project is at a very early stage. So, in this deliverable, as requested, answers to comments are provided together with an updated Ethical Self-Assessment.”<sup>6</sup>

### 3.2 Ethics Assessment

#### 3.2.1 Impact Assessment Architecture

The architecture for impact assessment generally comprises two key elements: the "framework" and the "method." In this context, a framework acts as the fundamental supporting structure or organisational arrangement for impact assessment policies. It defines and describes the conditions and principles governing the assessment process. On the other hand, a method refers to the specific procedures or approaches used in the practice of impact assessment. It outlines the consecutive and/or iterative actions necessary to carry out the assessment.

Numerous frameworks and methods for impact assessment already exist across various domains, each with differing applicability and quality. The ongoing demand for new frameworks and methods stems from the receptiveness principle of the impact assessment. This principle dictates that both the framework and the method must continuously improve to better serve the goals of the impact assessment. This includes learning from past experiences or the experiences of other evaluation techniques, adapting to societal changes, and accommodating new domains where an impact assessment is applied.

This section outlines the method to be utilised for ethical impact assessment within the GOVTECH4ALL project.

---

<sup>6</sup> GOVTECH4ALL Consortium, *Procedures on Ethics Requirements No.1*, (Brussels, 2023).



### 3.2.2 GOVTECH4ALL Impact Assessment Description

Conducting an impact assessments empowers private and public organisations to contemplate the consequences of their planned initiatives and identify ways to minimise or prevent negative and unintended outcomes before they emerge (like to an "early warning system"). This process yields benefits in terms of resource management and fosters public trust. An impact assessment is considered a "best-effort obligation" that serves as evidence of due diligence and accountability towards regulatory authorities. If conducted transparently, impact assessments facilitate public confidence by demonstrating an organisation's genuine concern for legal and ethical issues and their appropriate consideration.

The activities involved in the development and implementation of GOVTECH4ALL encompass various aspects, including data protection and privacy laws, ethical concerns, and societal acceptance of GOVTECH4ALL approaches. Consequently, the impact assessment in GOVTECH4ALL will encompass all these areas and incorporate several types of assessments and relevant techniques.

The focal point of GOVTECH4ALL's impact assessment lies in evaluating the risks associated with the rights and freedoms of natural persons concerning the processing of their personal data in the project.

It is important to note that privacy and data protection, while related, are not identical concepts. Therefore, the Data Protection Impact Assessment (DPIA) does not include a privacy impact assessment, which will be carried out as part of the overall impact assessment for the project (see section 7.6). Overall, the described elements of the impact assessment in GOVTECH4ALL will encompass assessments of legal obligations, ethical considerations, and liability implications.

The primary parameters of GOVTECH4ALL's Impact Assessment are as follows:

- a) Ensuring compliance with the legal requirements of the GDPR.
- b) Safeguarding the fundamental rights, including privacy, of civil servants and other involved subjects.
- c) Ensuring societal acceptance and trust in GOVTECH4ALL activities.
- d) Addressing ethical concerns related to GOVTECH4ALL.

### 3.2.3 Impact Assessment Methodology

The following section delineates the means of performing an impact assessment that encompasses diverse methodologies, with no universally applicable solution. The appropriateness of a particular methodology relies on various factors, including the industry, context, as well as social, legal, and cultural considerations. For practicality, impact assessments must possess scalability, flexibility, and adaptability to cater to organisations of all sizes and sectors.

For an impact assessment to be effective, it must be built upon well-defined goals and principles. In the case of the GOVTECH4ALL project, the scenario involves a pre-use assessment, relying on expected uses, actual simulations, and tests conducted throughout the project's research duration.

The overall impact assessment methodology hinges upon the establishment of a clear framework for each project partner's involvement. This chosen approach should empower partners to make informed decisions concerning project risks, ensuring compliance with legal and ethical requirements while garnering societal acceptance.



This project has received funding from the European Union's Horizon Europe Framework Programme under grant agreement N° 101057497.

The Impact Assessment Methodology used in GOVTECH4ALL mirrors the project's goals, features, and context, accommodating the specific needs of its partners. It unfolds in five distinct phases, comprising eleven essential actions (seven consecutive, three spanning the entire process, and one revisited at M24):

- i) Phase I: Preparation of the assessment process
  - (1) Action 1: Screening
  - (2) Action 2: Scoping
  - (3) Action 3: Planning and preparation
- ii) Phase II: Assessment
  - (1) Action 4: Description
  - (2) Action 5: Assessing the necessity and proportionality of the relevant operations
  - (3) Action 6: Identification, analysis, and assessment of relevant risks for the rights and freedoms of concerned subjects
- iii) Phase III: Recommendations
  - (1) Action 7: Recommendations
- iv) Phase IV: On-going actions
  - (1) Action 8: Stakeholder consultation/involvement
  - (2) Action 9: Documentation and drafting the GOVTECH4ALL report
  - (3) Action 10: Quality control
- v) Phase V: Maintenance
  - (1) Action 11: Monitoring and observance reports (M12 and M24)

This structured methodology allows for a comprehensive evaluation of impacts while ensuring that the GOVTECH4ALL project aligns with its objectives and responsibilities."

### 3.3 Impact Assessment Requirements

#### 3.3.1 GDPR framework and DPIA

##### 3.3.1.1 Data Protection Impact Assessment

Since May 25<sup>th</sup> 2018, GDPR<sup>7</sup> applies to all EU member states. One of main elements of GDPR, introduced in Article 35, is the need to perform a Data Protection Impact Assessment (DPIA) in specific situations.

Although not specifically described in GDPR, DPIA is considered as a process designed to describe the data processing and assess its necessity and proportionality. The DPIA is designed to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation<sup>8</sup>. Put simply, a DPIA is a procedural step to establish and showcase compliance, aiming to prevent potential repercussions of non-compliance, which could incur fines of up to 4% of a company's worldwide turnover.

---

<sup>7</sup> 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).

<sup>8</sup> See also recital 84: "The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation".



This project has received funding from the European Union's Horizon Europe Framework Programme under grant agreement N° 101057497.

The GDPR places obligations on both:

- the 'data controller', which 'alone, or jointly with others, determines the purposes and means of the processing of personal data'; and
- the 'data processor', which 'processes personal data on behalf of the controller'.

However, the subject responsible for carrying out of DPIA is the data controller.<sup>9</sup> If the processing is wholly or partly performed by a data processor, the processor should assist the controller in carrying out the DPIA and provide any necessary information.<sup>10</sup>

The GOVTECH4ALL project, team is applying the regulation defined by the Commission "[Ethics and data protection](#)<sup>11</sup>" as mandatory for all EU projects. The Consortium will ensure that any partners, contractors or service providers that process research data at our request and on our behalf comply with the GDPR and the EU ethics standards.

### *3.3.1.2 When DPIA is required*

According to Guidelines on the DPIA (wp248 rev.01)<sup>12</sup>, a DPIA is mandatory in certain situations while it is only suggested in others; in particular, it is mandatory when the process is "likely to result in a high risk". It is also encouraged in situations where its necessity is unclear: "In cases where it is not clear whether a DPIA is required, the European Data Protection Board<sup>13</sup> recommends that a DPIA is carried out nonetheless as a DPIA is a useful tool to help controllers comply with data protection law".

Article 35(3)<sup>14</sup> provides some examples of situations warranting a mandatory DPIA, when a processing operation is "likely to result in high risks":

- "a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- processing on a large scale of special categories of data referred to in Article 9(1)<sup>15</sup>, or of
- personal data relating to criminal convictions and offences referred to in Articles 10<sup>16</sup>; or
- a systematic monitoring of a publicly accessible area on a large scale".
- Additionally, the WP29 Guidelines provide the following criteria that shall be considered to define the need for DPIA:<sup>17</sup>
  1. Evaluation or scoring
  2. Automated-decision making with legal or similar significant effect
  3. Systematic monitoring
  4. Data processed on a large scale
  5. Sensitive data or data of a highly personal nature
  6. Matching or combining datasets
  7. Data concerning vulnerable data subjects

<sup>9</sup> WP29.

<sup>10</sup> Ibid

<sup>11</sup> [https://ec.europa.eu/research/participants/data/ref/h2020/grants\\_manual/hi/ethics/h2020\\_hi\\_ethics-data-protection\\_en.pdf](https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf)

<sup>12</sup> [http://ec.europa.eu/newsroom/document.cfm?doc\\_id=47711](http://ec.europa.eu/newsroom/document.cfm?doc_id=47711)

<sup>13</sup> <https://edpb.europa.eu/>

<sup>14</sup> <https://gdpr-info.eu/art-35-gdpr/>

<sup>15</sup> <https://gdpr-info.eu/art-9-gdpr/>

<sup>16</sup> <https://gdpr-info.eu/art-10-gdpr/>

<sup>17</sup> WP29 Guidelines



8. Innovative use or applying new technological or organisational solutions
9. When the processing in itself “prevents data subjects from exercising a right or using a service or a contract”

The need to conduct a DPIA in GOVTECH4ALL is explained in the following section with regard to applicability of the criteria mentioned above to GOVTECH4ALL activities.

### 3.3.1.4 Why have a DPIA in GOVTECH4ALL

Although the project is not running “systematic” actions as described in GDPR regulation, being a research project in which some pilots will run for a limited period of time in a contained space, some actions carried out (e.g stakeholder profiling, etc.) could partially go under some of criteria specified in section 3.1.

For instance, one criterion for the large-scale definition is the proportion of an area monitored, which could be close to 100% on a GOVTECH4ALL pilot site with public administration bodies directly involved.

In view of these, we suggested all partners involved as data controller to complete a dynamic DPIA. In the early months of the project this is considered to be preliminary, as there is not yet a detailed view of data use along the project.

Furthermore, there is a specific point stating: “Innovative use or applying new technological or organisational solutions, like combining use of fingerprint and facial recognition for improved physical access control, etc. The GDPR makes it clear (Article 35 and recitals 89<sup>18</sup> and 91<sup>19</sup>) that the use of a new technology, defined in “accordance with the achieved state of technological knowledge” (recital 91), can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals’ rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will support the data controller in understanding the risks therein and how to address such risks. For example, certain “Internet of Things” applications could have a significant impact on individuals’ daily lives and privacy; and therefore, require a DPIA”.

Moreover, some of the DPIA criteria might be applicable to GOVTECH4ALL, as explained below in Table 3-1 - DPIA criteria:

GOVTECH4ALL processing	Possible relevant criteria	DPIA needed
The use of camera systems to monitor citizens’ behaviour.	<ul style="list-style-type: none"> <li>- Systematic monitoring.</li> <li>- Innovative use or applying technological or organisational solutions</li> </ul>	YES
The gathering of public social media data for generating scenarios and defining context.	<ul style="list-style-type: none"> <li>- Evaluation or scoring</li> <li>- Data processed on a large scale</li> <li>- Matching or combining of datasets</li> </ul>	YES

<sup>18</sup> <https://gdpr-info.eu/recitals/no-89/>

<sup>19</sup> <https://gdpr-info.eu/recitals/no-91/>

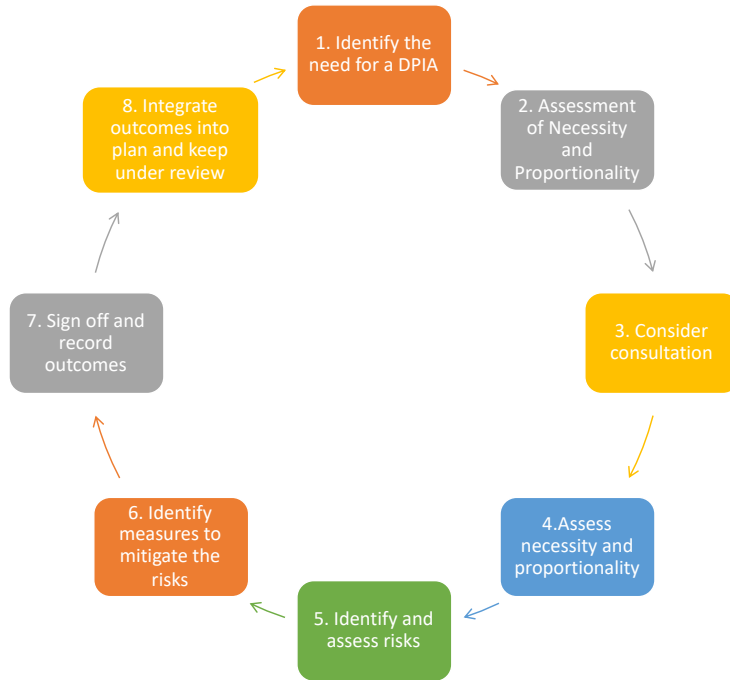


The processing of health data.	<ul style="list-style-type: none"> <li>- Sensitive data or data of a highly personal nature</li> <li>- Data processed on a large-scale</li> </ul>	YES
--------------------------------	---	-----

**Table 3-1 - DPIA criteria**

**3.3.1.5 DPIA process key elements**

A DPIA should begin early in the life of a project, before processing commences, and run alongside the planning and development process. The UK’s Information’s Commissioner Officer diagram<sup>20</sup>, shown in Figure 3-1 - DPIA assessment process, illustrates the main actions:



**Figure 3-1 - DPIA assessment process**

A more detailed description of the steps is provided below:<sup>21</sup>

STEP	COMPLIANCE CHECK
<b>1: Identify for each single partner the need for a DPIA</b>	The criteria to define whether the DPIA is applicable to GOVTECH4ALL are described in sections 3.1. The consultation of the organisation’s GDPR compliance structure (a DPO if appointed), is also strongly suggested.
	Partners’ law compliance and transparency Conduct an information audit to determine what information is processed and who has access to it. Each GOVTECH4ALL partner has a legal justification for any data processing activities. Each partner provides clear information about data processing and legal justification in the privacy policy.
	Data security managed by each single GOVTECH4ALL partner Take data protection into account at all times, from the moment organisations begin developing a

<sup>20</sup> <https://ico.org.uk/>

<sup>21</sup>ICO: Guideline to GDPR - <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/>



This project has received funding from the European Union’s Horizon Europe Framework Programme under grant agreement N° 101057497.

	<p>product to each time it processes data appointing a proper monitoring procedure.</p> <p>Encrypt, pseudonymise, or anonymise personal data wherever possible (take care in particular of all biometric and health related data going to be used by GOVTECH4ALL partners).</p> <p>Each partner creates an internal security policy for research team members and build awareness about data protection.</p> <p>Know when to conduct a DPIA and have a process in place to carry it out.</p> <p>Have a process in place to notify the authorities and your data subjects in the event of a data breach.</p>
Accountability and governance	<p>Each partner should designate someone responsible for ensuring GDPR compliance across the organisation.</p> <p>Appoint, if necessary, a Data Protection Officer</p>
Privacy rights	<p>It's easy for GOVTECH4ALL stakeholders (internal/external)</p> <ul style="list-style-type: none"> <li>• to request and receive all the information you have about them.</li> <li>• to correct or update inaccurate or incomplete information<sup>22</sup>.</li> <li>• to request to have their personal data deleted.</li> <li>• to ask you to stop processing their data.</li> <li>• to receive a copy of their personal data.</li> <li>• For partners process their data.</li> </ul> <p>If one of GOVTECH4ALL's module makes decisions about people based on automated processes, stakeholders have a procedure to protect their rights.</p>
	<p>When GOVTECH4ALL partners do this screening and decide a DPIA is not needed, they should document their decision and the reasons for it. In case of doubt, completing a DPIA is suggested.</p>
<b>Step 2: Each partner should describe the processing</b>	<p>In order to provide a clear view of processes as required by art. 35.7<sup>23</sup>, and to enhance the compliance with GDPR principles a DPIA should be carried out <u>before processing data</u> due the lack of that could generate high risks for the organisation. See Recitals 84<sup>24</sup>,90<sup>25</sup> and 94<sup>26</sup></p>

<sup>22</sup> Art. 15 and 16 - The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data..., The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her....

<sup>23</sup> Art.35(7)(a): a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller.

<sup>24</sup> Recital 84: In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk.

<sup>25</sup> Recital 90: In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk

<sup>26</sup> Recital 94: Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities.





	The nature of the processing	<ul style="list-style-type: none"> <li>• how data is <ul style="list-style-type: none"> <li>○ collected;</li> <li>○ stored;</li> <li>○ used</li> </ul> </li> <li>• who <ul style="list-style-type: none"> <li>○ has access to the data;</li> <li>○ do you share the data with;</li> </ul> </li> <li>• whether partners use any processors;</li> <li>• retention periods;</li> <li>• security measures;</li> <li>• whether partners use any new technologies;</li> <li>• novel types of processing; and</li> <li>• which screening criteria has been flagged as likely high risk.</li> </ul>
	The scope of the processing	<p>Related to personal data:</p> <ul style="list-style-type: none"> <li>• the nature of them;</li> <li>• the volume and variety;</li> <li>• The sensitivity.</li> </ul> <p>Related to their processing:</p> <ul style="list-style-type: none"> <li>• extent and frequency;</li> <li>• duration;</li> <li>• number of data subjects involved;</li> <li>• Geographical area covered.</li> </ul>
	The context of the processing	<ul style="list-style-type: none"> <li>• the source of the data;</li> <li>• the nature of partner relationship with the individuals;</li> <li>• the extent individuals have control over their data;</li> <li>• for how long individuals are likely to expect the processing;</li> <li>• whether these individuals include children or other vulnerable people (not the case in GOVTECH4ALL although when collecting data from autonomous vehicles there is the possibility to have those categories partially included);</li> <li>• any previous experience of this type of processing;</li> <li>• any relevant advances in technology or security;</li> <li>• any current issues of public concern; in due course, whether you comply with any GDPR codes of conduct (once any have been approved under Article 40<sup>27</sup>) or GDPR certification schemes;</li> </ul>

<sup>27</sup> Art. 40 - <http://www.privacy-regulation.eu/en/article-40-codes-of-conduct-GDPR.htm>



		<ul style="list-style-type: none"> <li>• Whether compliance with relevant codes of practice has been considered.</li> </ul>
	The purpose of the processing	<ul style="list-style-type: none"> <li>• Partner legitimate interests, where relevant;</li> <li>• the intended outcome for individuals;</li> <li>• the expected benefits for the partner, the project or for society as a whole.</li> </ul>
	During GOVTECH4ALL's lifetime, and starting from the release of D2.3, this step will achieve a very high importance and the methodology provided herein could facilitate the identification of potential issues to be addressed by a DPIA.	
<b>Step 3: Partners should consider consultation</b>	In case of doubts, each partner can consult his country privacy agency to receive suggestions and be supported in the assessment procedures.	
<b>Step 4: Each partner should assess necessity and proportionality</b>	<p>Due to the fact that GOVTECH4ALL is working with data related to citizens and their health, a clear identification of the purposes of the processing operation (specific, explicit and legitimate) should be addressed as stated in recital 39 of the GDPR<sup>28</sup>. On the other hand, a timeline and justification of data use should be provided compared with the evidence of possible alternative ways to conduct the data collection and its analysis.</p> <p>Anyhow data collected should be adequate, relevant and limited to what is strictly necessary in relation to the purposes for which the data are processed (data minimisation principle), see Art. 5 of the GDPR<sup>29</sup></p> <p>Data should also be accurate and kept up to date (accuracy principle).</p> <p>Furthermore, data retention principles should be explicated (storage principle) with a clear indication of expiring policy and related data deleted.</p>	
<b>Step 5: Each partner should identify and assess risks</b>	<p>At this stage, it is necessary to consider the potential impact on individuals and any harm or damage the processing may cause – whether physical, emotional, or material. GOVTECH4ALL will apply the following methods to identify and assess risks (also described in more detail in chapter 4 herein).</p> <ul style="list-style-type: none"> <li>• Baseline security criteria: the minimum set of defences to fend off risks;</li> <li>• Risk scale: a universal way of quantifying risk;</li> <li>• Risk appetite: the level of risk the organisation is willing to accept; and</li> <li>• Scenario- or asset-based risk management: the strategies to reduce the damage caused by certain incidents or that can be caused to certain parts of the organisation.</li> </ul> <p>Furthermore Art. 32 requires risks “from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data” to be identified and mitigated.</p>	
<b>Step 6: Each partner should identify measures to mitigate the risks</b>	<p>All the sources of the identified risks shall be recorded. Moreover, for all the risks the measures to avoid or minimise them shall be considered. At this stage of the GOVTECH4ALL project at least the following measures might be identified: Take measures to pseudonymise and encrypt personal data;</p> <ul style="list-style-type: none"> <li>• Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;</li> </ul>	

<sup>28</sup> Rec. 39 - Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed.

<sup>29</sup> Art. 5 - Principles relating to processing of personal data.



	<ul style="list-style-type: none"> <li>• Restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and/or</li> <li>• Implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.</li> </ul>
<b>Step 7: Final step, process closing and outcomes recorded</b>	The primary aim of conducting a DPIA is to identify and minimise the data protection risks involved in a project. However, as has been emphasised throughout this guide, keeping a record of all steps taken as part of the DPIA will help to ensure that the process is completed thoroughly, and to reassure stakeholders that all data protection risks have been considered. This written record should also form the basis of putting into effect the data protection solutions which have been identified, and can be used to check off the implementation of each solution. The GOVTECH4ALL project is providing a dynamic tool to manage DPIA evolution during project lifecycle.
<b>Step 8: Integrate outcomes into plan and keep under review</b>	After completing the process, each partner should integrate the outcomes from his DPIA back into GOVTECH4ALL project plan, and keep his DPIA under review using the wiki tool provided by the GOVTECH4ALL team. Throughout this process, each partner should consult individuals and other stakeholders as needed.

The methodology proposes an innovative approach, based on the use of a dedicated online monitoring tool, to the DPIA that is closely related to processes in place in executing the GOVTECH4ALL project and considering the expected outcomes and risks associated with those actions.<sup>30</sup>

The main goal is to provide GOVTECH4ALL's partners with tools to conduct an effective DPIA.

### 3.3.2 The dynamic compliance process

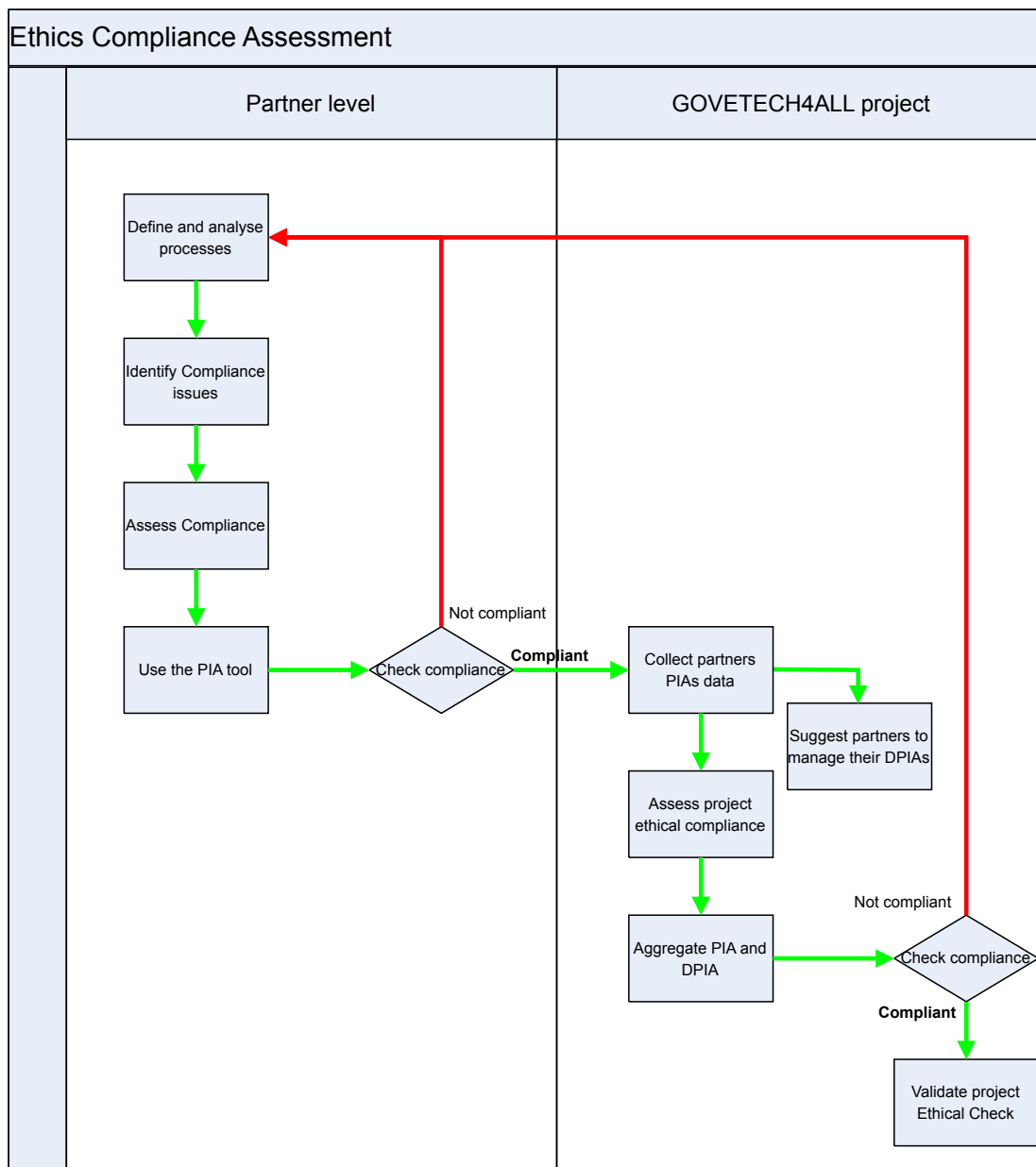
Once the first Impact assessment and the related DPIA has been completed, the dynamic compliance process will start, supported by the wiki tool provided by the GOVTECH4ALL project.

Being a research project GOVTECH4ALL, needs to have a harmonised view to drive its overall impact. In view of that, here an extension of single partner compliance assessment process is proposed.

The graph in **Error! Reference source not found.**, presents the various steps each partner should follow to achieve the compliance assessment.

<sup>30</sup> Duricu, Alexandra (2019). Data Protection Impact Assessment (DPIA) and Risk Assessment in the context of the General Data Protection Regulation (GDPR).





**Figure 3-2 – Ethical Compliance assessment process**

As result of analysis, compliance issues are going to be identified and assessed in terms of risks and action to be planned. The following step will be the use of the DPIA tool accessible through the “confluence” area to report the compliance strategy inside the single partner DPIA. Periodically, a compliance check will be performed to keep the DPIA updated. Once each individual partner’s DPIA is completed, data are transferred to the overall project compliance check, where harmonisation action will be activated and the overall picture will be verified in terms of compliance with regulation.

After that check the GOVTECH4ALL project DPIA will be ready to be published and periodically it will be verified and updated according to possible changes in the use/collection of data occurred during the project lifecycle. In the case of not compliance both at each partner as at project level, the entire process should be revised.



Each GOVTECH4ALL partner is able keep his compliance updated using the tools described in section 4 of this document following the process described in section 7.6.

### 3.3.3 Other Legal Obligations Impact Assessment

The GOVTECH4ALL legal impact assessment includes various components, such as the DPIA and an examination of privacy impacts. These assessments will be conducted using the general impact assessment methodology employed in the project.

While not mandated by legislation, the privacy impact assessment (PIA) remains a valuable tool for GOVTECH4ALL partners to explore the applicability of privacy frameworks to their operations, evaluate associated risks, and develop measures to prevent or minimise them. The PIA will focus on areas not covered by the DPIA, specifically addressing privacy concerns that may not directly affect data protection rights. By doing so, it ensures compliance with privacy laws and helps public trust in the development and implementation of GOVTECH4ALL. The project's privacy by design approach should aid in addressing these specific issues.

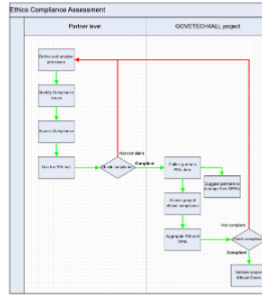
All the mentioned types of legal obligation impact assessments, including DPIA, will enable GOVTECH4ALL's partners to proactively avoid legal liabilities and other adverse consequences resulting from non-compliance.

### 3.3.4 Online Monitoring Tool

To provide GOVTECH4ALL partners with a unique reference point to manage ethical issue and provide information for the dynamic ethical assessments, a dedicated environment in a “confluence” space has been created and all partners have access to that to keep their data updated and to open discussions on potential ethical issues that could arise during the project.

- The environment presents, in the beginning, the overall Ethical Compliance Assessment process.
- An area is dedicated to collect work done in terms of periodic/initial Ethics Screening with results collected in related surveys involving all partners.
- The following area collects datasets used in the project activities using the provided (see 7.6) template with the possibility to manage versioning of data sets.
- The environment then gives access to the PIA tool allowing for an assessment managed by each partner.
- A “Trello” board provides the tasks management for planned activities.
- A Gantt chart provides an updated view of activities status.
- Several blog streams are supported to open discussions among partners and co-elaborate strategies to face potential ethical issues.





**Welcome in the Ethics Advisor Area Overview**

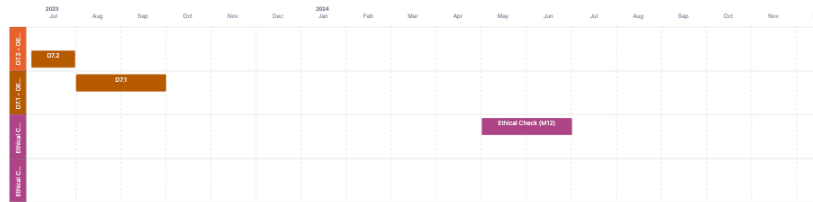
- In this area you could find activities performed by the Advisor and interact dynamically to assess project Ethical Requirements.
- Have direct links to the first surveying page:
  - Comments to Ethics Screening Survey 1
  - Ethics Screening Survey 1 results

**Data Sets**

- In this area you could find activities related to **Data Sets collection**.
- Please use the following template for each data set and **send completed ones** to the Ethics team:
  - Dataset template
- Here you can find collected Data Sets (to be updated if changes occurred):
  - Dataset LC 01 (xx-yy-zzzz)

**DPIA Management area**

- In this area you could find the link to PIA tool developed by CNIL in France that could support the creation of your DPIA. If you have your internal procedure you are free to use that.
- Furthermore you can find a link to a project oriented template that could be used to generate your own PIA:
  - PIA tool download
  - PIA template download



**Figure 3-3 – Online Monitoring Tool**



This project has received funding from the European Union’s Horizon Europe Framework Programme under grant agreement N° 101057497.

## 4. Conclusions

In conclusion, Deliverable 7.1 represents a pivotal resource in the GOVTECH4ALL project, presenting the meticulously crafted Ethics Strategy. This framework stands as a robust foundation for the continuous ethical assessment integral to the progression of the project. In strict adherence to the directives of the Specific Grant Agreement, which emphasise the sustained infusion of ethical considerations, this strategy steers the course of the GOVTECH4ALL consortium activities in ethics, responsible innovation, and technology application. The document is structured into four pivotal sections: an introductory discourse on the nexus of ethics and technology, an exhaustive explication of pertinent clauses within the Specific Grant Agreement and associated documents, overarching guiding principles, the central strategy, and concluding insights. Additionally, an Annex supplements this document, offering templates and tools instrumental in the consortium's implementation of this strategy.



This project has received funding from the European Union's Horizon Europe Framework Programme under grant agreement N° 101057497.

## Reference List

GOVTECH4ALL Consortium, Specific Grant Agreement, (Brussels, 2023).

GOVTECH4ALL Consortium, Validation Framework and Maturity Assessment, Brussels (2023).

GOVTECH4ALL Consortium, Procedures on Ethics Requirements No.1, (Brussels, 2023).

Duricu, Alexandra, *Data Protection Impact Assessment (DPIA) and Risk Assessment in the context of the General Data Protection Regulation (GDPR)*, (Lulea, 2019).

European Parliament and Council of the European Union, *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*, (Brussels, 2016).



This project has received funding from the European Union's Horizon Europe Framework Programme under grant agreement N° 101057497.



## Annex A - Dataset description template

Although in this project a data management plan was not planned to give better possibility for a sound ethical assessment, all partners will be requested to complete the following template for each data set that could include direct or indirect personal data.

Dataset Name		
Partner who filled the table:		
Data Summary	Brief description:	
	Reused data (yes/no, why)?	
	Type of data (E.g.: Sample or specimen data, Observational, Experimental, Simulation, Derived or compiled, other, ...):	
	Format of data (E.g.: gif, jpeg, mpeg, mp3, 3D Studio, ...)	
	Purpose and relation to project objectives:	
	Size of dataset:	
	Origin/provenance of data:	
	To whom it might be useful (Researchers, Research communities, Decision Makers, Education, Economy, The Public, Industry, Other)?	
FAIR Data: Making data findable	Is data identified by a persistent identifier? Which?	
	Is rich metadata provided to allow discovery? What metadata will be created?	
	Are search keywords provided?	
	Is metadata harvesting and indexing possibility be offered?	
FAIR Data: Making data accessible	Repository	Which trusted repository is used (if any)?
		Are there arrangements with the repository



	D a t a	Is data made openly available (Yes/No, Why)?	
		Is an embargo applied to this (Yes/No, How Long, Why)?	
		Are there methods/tools/protocols needed to access it (Yes/No, Which, Why)?	
		Are there restrictions on use? How access will be provided during and after the project ends? How will identity of persons be ascertained?	
	M e t a d a t a	Are metadata made openly available and licenced under a public domain dedication CC0, as per the Grant Agreement (Yes/No, Why)?	
		Do metadata contain information to enable the user to access the data?	
		How long will the data remain available and findable? Will metadata be guaranteed to remain available after data is no longer available?	
FAIR Data: Making data interop erable	Are standard controlled vocabularies used in metadata?		
	If you created the vocabulary, where can it be found? Is there a mapping to commonly used ontologies?		
	Are there qualified references to other data?		
FAIR Data: increas e data reuse	Is there documentation to validate data analysis? Which? (E.g.: readme file)?		
	Is data available in the public domain? Under which Licence (See Art. 17 of the Grant Agreement)		
	In case of data produced in the project: can data be used by third parties after the project ends?		
	Is data provenance well documented (Yes/No, How)?		
	Which relevant data quality assurance processes were used?		
Allocat ion of	What is the cost of making the described output FAIR?		



resources	How is this covered?	
	Who is the person responsible for the management of this dataset?	
	Is long term preservation guaranteed for this? How?	
Security	What security measures are followed (E.g.: Encryption, Hash codes, firewalls, access control, ...)?	
	What conditions do the security measure meet (E.g.: Data Access, Data backup/recovery, ...)?	
Ethics	Are there any ethical or legal issues that can have an impact on sharing the described dataset (Yes/No, Why)?	
	Does the described dataset contain sensitive information. (Yes/No/Why)?	
	<b>Is a Data Protection Impact Assessment (DPIA) needed? (Yes/No/Why)?</b>	
	Does the described dataset contain personal data (Yes/No/Why)?	
	What are the methods used for processing and accessing sensitive/personal information (E.g.: Anonymisation, Privacy constraints, Informed Consent statements, Privacy policies, National laws)	
Other issues	Do you make use of other procedures for data management (Yes/No/Which)?	

## Annex B - GAP analysis and DPIA generation tool and template

To facilitate the privacy impact assessment, we propose to all partner the use of the free available software provided by the **French Data Protection Authority (CNIL)** that is meant to guide the data controllers in building and demonstrating compliance to the GDPR. It helps to properly carry out a data protection impact assessment by facilitating the use of the PIA method developed by the CNIL.

Here follow some screens used to proceed in the entire process.

The first area is the CONTEXT:



This project has received funding from the European Union's Horizon Europe Framework Programme under grant agreement N° 101057497.



## Context

This section gives you a clear view of the treatment(s) of personal data in question.

### OVERVIEW

*This part allows you to identify and present the object of the study.*

#### What is the processing under consideration? ^

Govtech4all-beta is the first implementation of Govtech4all Framework Partnership Agreement. As its name shows, it is an experiment of new ways to deliver public sector innovation, based on collaboration with innovative players such as startups and between government agencies, embracing the “agile” concept by design. The goal is to open the public sector technology market to ensure that governments use the best solutions - not those that better fit procurement processes or that suffer from the “not invented here” syndrome. Govtech4all-beta brings together 14 govtech European key players from 10 countries in order to foster a single EU govtech market, and promote new models of public sector innovation. In the project, public and private sector, research bodies and NGOs will work together to learn from each other, deliver common pilots and raise the profile of govtech in each country and at EU level. Concretely, the project central focus is the delivery of three pilots, through startup challenges, in-house development, and innovative procurement.

#### What are the responsibilities linked to the processing? ^

Privacy and security are two of the major pillars of data sharing intermediaries in public administration and European Data Spaces, particularly in light of rapid digitization and global economic and sociopolitical trends, recently accelerated by the COVID19 pandemics, remote working and intensification of digital communication. To allow a secure, trustworthy, and sustainable data economy, both new national/cross-border initiatives on privacy and security enhancement, and novel research breakthroughs and the potential of privacy-preserving technology must be enabled to comply with data protection law such as the GDPR

#### Are there standards applicable to the processing? ^

*List the relevant standards applicable to the processing, especially approved codes of conduct and data protection certifications.*



This project has received funding from the European Union’s Horizon Europe Framework Programme under grant agreement N° 101057497.

## What are the data processed? ^

**Set out a detailed list of the data processed, by category, and persons with access thereto.**

For example:

### **Information about the user**

- first name
- date of birth
- gender
- email
- telephone number

*Common data:* identification data

*Recipients:* host

*Persons with access thereto:* authorized staff at host and manufacturer

### **Data entered in a third-party app**

obtained via a link with the user account

*Common data:* identification data

*Recipients:* host

*Persons with access thereto:* authorized staff at host and manufacturer

### **Recorded data**

- texts/messages
- sounds/images/movements
- temperature/humidity
- user logs on the device, mobile app and online service

*Common data:* life habits

*Data perceived as sensitive:* image and voice (enabling biometric processing)

*Sensitive data (in the meaning of the GDPR):* data relating to minors

*Recipients:* host, interactivity and advertising providers

*Persons with access thereto:* authorized staff at the different firms

### **Calculated data**

- answers to children's questions
- identification of interests to help make answers more relevant
- analysis of uses
- targeted advertising

*Common data:* life habits

*Sensitive data (in the meaning of the GDPR):* data relating to minors

*Recipients:* host, interactivity and advertising providers

*Persons with access thereto:* authorized staff at the different firms



This project has received funding from the European Union's Horizon Europe Framework Programme under grant agreement N° 101057497.

## How does the life cycle of data and processes work? ^

Present a detailed description of the processes carried out.

For example:

1. **Open an account:** the user provides identification data to open his or her account
2. **Capture the data:** data are recorded via sensors
3. **Transfer to the mobile:** the data are transferred to the mobile app, directly via the device or through the cloud servers
4. **Enter the data:** data are entered into the mobile app
5. **Store in the mobile:** the data are stored in the mobile app
6. **Send the data to the servers:** the data are sent to the cloud servers, via the device directly or the mobile app
7. **Generate interactivity:** the interactive platform in the cloud generates the response data on the basis of previous dialogues and the interests detected
8. **Send the data to the toy:** the interactive data are sent back to the device, directly or through the mobile app
9. **Store the data on the servers:** the captured and calculated data are stored on the cloud servers
10. **Analyze the data:** data analysis algorithms are run on the cloud servers to produce statistics on use and advertising targeting
11. **Consult the cloud server data:** part of the captured and calculated data can be consulted via the mobile app or on a personal Web space
12. **Share the data:** some data can be passed on to third-party apps or posted on social media websites

## How does the life cycle of data and processes work? ^

Present a detailed description of the processes carried out.


For example:

1. **Open an account:** the user provides identification data to open his or her account
2. **Capture the data:** data are recorded via sensors
3. **Transfer to the mobile:** the data are transferred to the mobile app, directly via the device or through the cloud servers
4. **Enter the data:** data are entered into the mobile app
5. **Store in the mobile:** the data are stored in the mobile app
6. **Send the data to the servers:** the data are sent to the cloud servers, via the device directly or the mobile app
7. **Generate interactivity:** the interactive platform in the cloud generates the response data on the basis of previous dialogues and the interests detected
8. **Send the data to the toy:** the interactive data are sent back to the device, directly or through the mobile app
9. **Store the data on the servers:** the captured and calculated data are stored on the cloud servers
10. **Analyze the data:** data analysis algorithms are run on the cloud servers to produce statistics on use and advertising targeting
11. **Consult the cloud server data:** part of the captured and calculated data can be consulted via the mobile app or on a personal Web space
12. **Share the data:** some data can be passed on to third-party apps or posted on social media websites



This project has received funding from the European Union's Horizon Europe Framework Programme under grant agreement N° 101057497.

Then fundamental principles are addressed



## Fundamental principles

This section allows you to build the compliance framework for privacy principles.

### PROPORTIONALITY AND NECESSITY

*This part allows you to demonstrate that you are implementing the necessary means to enable the persons concerned to exercise their rights.*

Are the processing purposes specified, explicit and legitimate? ^

*Explain why the processing purposes are specified, explicit and legitimate.*

What are the legal basis making the processing lawful? ^

**Article 35 GDPR**

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.
3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:
  - a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
  - processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
  - a systematic monitoring of a publicly accessible area on a large scale.



This project has received funding from the European Union's Horizon Europe Framework Programme under grant agreement N° 101057497.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.
5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.
6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.
7. The assessment shall contain at least:
- (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
  - (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
  - (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
  - (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.
8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.
9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.
10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.
11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.





Are the data collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')? ^

Present a detailed list of the data processed, reduced to what is strictly necessary, alongside the justification of the need and any additional minimization controls.

#### 1. Common data

**Civil status, identity, identification data:**

- **Details:** First name, date of birth, email, telephone number, link with a social media account
- **Justification:** details necessary for creating a profile for communicating
- **Minimization controls:**
  - No surname
  - Replacing the date of birth with the age or age group
  - Separate storage of identifying data in an encrypted base

**Personal life** (*living habits, marital status, excluding sensitive or dangerous data, etc.*):

- **Details:** Texts/messages, sounds, images, movements, temperature, humidity, answers to children's questions and identification of interests to help make answers more relevant, targeted advertising
- **Justification:** Aspects that are part of the communication features
- **Minimization controls:** No

**Professional life** (*résumé, education and professional training, awards, etc.*): Not collected

**Economic and financial information** (*income, financial situation, tax situation, etc.*): Non collectées

**Connection data** (*IP addresses, events logs, etc.*):

- **Details:** Application traces, technical logs
- **Justification:** Required for security reasons and to check compliance with the ST&Cs
- **Minimization controls:**
  - Pseudonymization for statistical use

**Location data** (*travels, GPS data, GSM data, etc.*):

- **Details:** Smartphone location integrated in the photos (if option is activated)
- **Justification:** not necessary
- **Minimization controls:**
  - Removal of location information before photos are sent

#### 2. Data perceived as sensitive

**Social security number:** Not collected

**Biometric data:**

- **Details:** Raw data, voice and photographs
- **Justification:** Aspects that are part of the communication features
- **Minimization controls:** No

**Bank data:** Not collected

#### 3. Sensitive data

**Opinions bearing on philosophy, politics, religion, trade union involvement, sexuality, health data, racial or ethnic origin, data concerning health or sexuality:**

- **Details:** Not collected but can appear directly or indirectly in the text, audio and video data
- **Justification:** Aspects that are part of the communication features
- **Minimization controls:** No

**Offences, convictions, security measures:** Not collected



This project has received funding from the European Union's Horizon Europe Framework Programme under grant agreement N° 101057497.

### Are the data accurate and kept up to date? ^

Set out in detail the data quality compliance controls, carried out on the device, the mobile app and the personal account, as well as a justification on the arrangements for or impossibility of implementing them.

Especially:

- Regular checks of the accuracy of the user's personal data
- Invitation for the user to check and, where necessary, update his or her data
- Traceability of data amendments

### What are the storage duration of the data? ^

*Explain why the storage durations are justified by legal requirements and/or processing needs.*

### How are the data subjects informed on the processing? ^

*Describe what is the information given to the data subjects and what are the means to do it.*

### If applicable, how is the consent of data subjects obtained? ^

*Describe the controls intended to ensure that users' consent has been obtained.*

### How can data subjects exercise their rights of access and to data portability? ^

Users rights concerning data collected:

**Right of access:**

- Data subjects can have access to their data upon simple email request to the DPO.

**Right to data portability:**

- All data collected are sent back to the data subject, they are available, before their deletion, upon simple request in CSV format.

### How can data subjects exercise their rights to rectification and erasure? ^

Data subjects can request to the DPO any change especially:

- Possibility of rectifying personal data
- Possibility of erasing personal data
- Indication of the personal data that will nevertheless be stored (technical requirements, legal obligations, etc.)
- Implementing the right to be forgotten for minors
- Clear indications and simple steps for erasing data before scrapping the device
- Advice given about resetting the device before selling it
- Possibility of erasing the data in the event the device is stolen



This project has received funding from the European Union's Horizon Europe Framework Programme under grant agreement N° 101057497.

### How can data subjects exercise their rights to restriction and to object? ^

Data subjects can verify asking the DPO the following:

- Existence of "Privacy" settings
- Existence of a system allowing the user to ask for the processing to be restricted
- Existence of technical means for the data controller to lock access to and use of the data subject to the restriction
- Effective exclusion of processing the user's data in the event consent is withdrawn

---

### Are the obligations of the processors clearly identified and governed by a contract? ^

Data could be processed only by Project 101121918 Govtech4all-beta

team members and all of them signed a Consortium Agreement specifying their obligations in terms of data processing.

Purpose of sharing is directly related to the research activity carried on in compliance with Art. 28 of GDPR.


---

### In the case of data transfer outside the European Union, are the data adequately protected? ^

**Data can circulate only in the EU and in the UK.**



The last input phase is related to risks





## Risks


This section allows you to assess the privacy risks, taking into account existing or planned controls.

**PLANNED OR EXISTING MEASURES**  
*This section allows you to identify controls (existing or planned) that contribute to data security.*

[+ Add an empty measure \(otherwise, use the knowledge base\)](#)

Encryption ^ 

Archiving ^ 

Website security ^ 



The PIA software performs a validation and then can printout the full DPIA.



This project has received funding from the European Union's Horizon Europe Framework Programme under grant agreement N° 101057497.

## Overview

### Fundamental principles

Purposes	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Legal basis	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Adequate data	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Data accuracy	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Storage duration	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Information for the data subjects	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Obtaining consent	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Right of access and to data portability	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Right to rectification and erasure	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Right to restriction and to object	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Subcontracting	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Transfers	<input type="checkbox"/>	<input checked="" type="checkbox"/>

### Planned or existing measures

<input type="checkbox"/>	<input checked="" type="checkbox"/>	Anonymisation
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Archiving

### Risks

<input type="checkbox"/>	<input checked="" type="checkbox"/>	Illegitimate access to data
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Unwanted modification of data
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Data disappearance

Improvable Measures  
Acceptable Measures

### Fundamental principles

No action plan recorded.

### Existing or planned measures

No action plan recorded.

### Risks

No action plan recorded.



This project has received funding from the European Union's Horizon Europe Framework Programme under grant agreement N° 101057497.



Deliverable D7.1

# Procedures on Ethics Requirements

## No.1

Work Package 7

Ethics

Version: Final



This project has received funding from the European Union's under specific grant agreement N° 101100457.