Project Acronym:	HosmartAI
Grant Agreement number:	101016834 (H2020-DT-2020-1 – Innovation Action)
Project Full Title:	Hospital Smart development based on AI

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101016834

DELIVERABLE

D8.2 – SELP Compliance Report

Dissemination level:	PU -Public
Type of deliverable:	R -Report
Contractual date of delivery:	31 August 2021
Deliverable leader:	VUB
Status - version, date:	Final – v1.0, 2021-08-31
Keywords:	Social, Ethical, and Legal Issues, SELP, Compliance, Impact assessment

This document is part of a project that has received funding from the European Union's Horizon 2020 research and innovation programme under agreement No 101016834. The content of this document reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains.
The document is the property of the HosmartAI consortium and shall not be distributed or reproduced without the approval of the HosmartAI Project Coordination Team. Find us at www.hosmartai.eu.

Executive Summary

The central question of this document, entitled D8.2 - SELP Compliance Report, is: what is the suggested Compliance Framework designed to address the relevant issues, to assess the impact of the technologies involved, and to comply with the regulatory framework relevant to HosmartAI. To address the question, it lays out the suggested framework, methodologies, and steps or processes of the Compliance Framework.

D8.2 builds upon previous task/deliverable T8.1/D8.1 which is a Benchmark Report of the relevant regulatory and ethical frameworks. D8.2 will be a basis for the next task/deliverable T8.3/D8.3 which is a SELP Impact Assessment.

The SELP Requirements are the specific standards or goals in practice that the Project needs to meet in the context of SELP. In other words, these SELP Requirements are the distilled version of the identified ethical, legal, and social issues and the relevant regulatory and ethical frameworks relevant to the Project.

When degerming the SELP Requirements, there is a number of important viewpoints or "principles." For example, they are not merely a transcription of the legal requirements; rather, they are re-written considering the operational aspect of compliance.

Furthermore, prioritizing SELP Requirements is an important aspect. We suggest using MoSCoW method to determine the priority.

Finally, this document elaborates the 7 (seven) steps for SELP Impact Assessment for HosmartAI. We suggest this model/cycle because we have used it in various projects in the past, and found it to be efficient and effective[1]. The processes are comprised of: (1) threshold analysis; (2) initiation of the assessment; (3) identification, characterisation, and description of the systems; (4) assessment; (5) stakeholder consultation; (6) risk management plan; (7) monitoring and reviewing.

[1] See Dariusz Kloza et al., Data protection impact assessment in the European Union: developing a template for a report from the assessment process (2020), https://osf.io/preprints/lawarxiv/7qrfp/; Dariusz Kloza et al., Towards a method for data protection impact assessment: Making sense of GDPR requirements (2020), https://osf.io/es8bm; Dariusz Kloza et al., Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals (2020), https://osf.io/b68em.

Deliverable leader:	Paul Quinn (VUB)
Contributors:	Hideyuki MATSUMI (VUB)
Reviewers:	Sofía Carbonell (HOPE), Marcela Chavez (CHUL)
Approved by:	Athanasios Poulakidas, Irene Diamantopoulou (INTRA)

Document History			
Version	**Date**	**Contributor(s)**	**Description**
0.1	2021-08-09	Hideyuki MATSUMI	Initial complete draft
0.2	2021-08-10	Hideyuki MATSUMI	Updated complete draft for internal peer review
0.3	2021-08-26	Hideyuki MATSUMI	Pre-final version addressing review comments
1.0	2021-08-31	A. Poulakidas, I. Diamantopoulou	Final version for submission

Table of Contents

Table of Figures

List of Tables

Definitions, Acronyms and Abbreviations

Acronym/ Abbreviation	Title
IA	Impact assessment
MoSoCoW	Must-haves, Should-haves, Could-haves, Won't haves
SELP	Social, ethical, and legal perspectives/issues

1 Introduction

1.1 Project Information

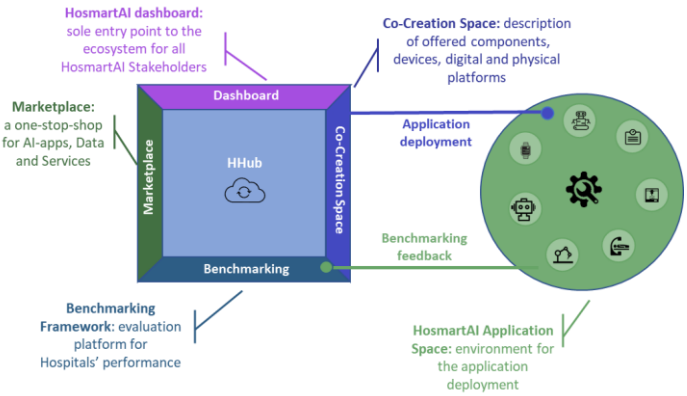
VISION

The HosmartAI vision is a strong, efficient, sustainable and resilient European **Healthcare system** benefiting from the capacities to generate impact of the technology European Stakeholders (SMEs, Research centres, Digital Hubs and Universities).

MISSION

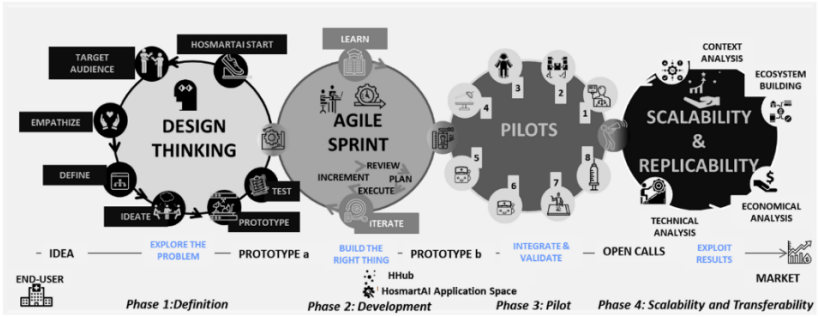
The HosmartAI mission is to guarantee the **integration** of Digital and Robot technologies in new Healthcare environments and the possibility to analyse their benefits by providing an **environment** where digital health care tool providers will be able to design and develop AI solutions as well as a space for the instantiation and deployment of a AI solutions.

HosmartAI will create a common open Integration **Platform** with the necessary tools to facilitate and measure the benefits of integrating digital technologies (robotics and AI) in the healthcare system.



A central **hub** will offer multifaceted lasting functionalities (Marketplace, Co-creation space, Benchmarking) to healthcare stakeholders, combined with a collection of methods, tools and solutions to integrate and deploy AI-enabled solutions. The **Benchmarking** tool will promote the adoption in new settings, while enabling a meeting place for technology providers and end-users.

Eight Large-Scale Pilots will implement and evaluate improvements in medical diagnosis, surgical interventions, prevention and treatment of diseases, and support for rehabilitation and long-term care in several Hospital and care settings. The project will target different **medical** aspects or manifestations such as Cancer (Pilot #1, #2 and #8); Gastrointestinal (GI) disorders (Pilot #1); Cardiovascular diseases (Pilot #1, #4, #5 and #7); Thoracic Disorders (Pilot #5); Neurological diseases (Pilot #3); Elderly Care and Neuropsychological Rehabilitation (Pilot #6); Fetal Growth Restriction (FGR) and Prematurity (Pilot #1).



To ensure a user-centred approach, harmonization in the process (e.g. regarding ethical aspects, standardization, and robustness both from a technical and social and healthcare perspective), the **living lab** methodology will be employed. HosmartAI will identify the appropriate instruments (**KPI**) that measure efficiency without undermining access or quality of care. Liaison and co-operation activities with relevant stakeholders and **open calls** will enable ecosystem building and industrial clustering.

HosmartAI brings together a **consortium** of leading organizations (3 large enterprises, 8 SMEs, 5 hospitals, 4 universities, 2 research centres and 2 associations – see Table 1) along with several more committed organizations (Letters of Support provided).

Table 1: The HosmartAI consortium.

Number[2]	Name	Short name
1 (CO)	INTRASOFT INTERNATIONAL SA	**INTRA**
1.1 (TP)	INTRASOFT INTERNATIONAL SA	**INTRA-LU**
2	PHILIPS MEDICAL SYSTEMS NEDERLAND BV	**PHILIPS**
3	VIMAR SPA	**VIMAR**
4	GREEN COMMUNICATIONS SAS	**GC**
5	TELEMATIC MEDICAL APPLICATIONS EMPORIA KAI ANAPTIXI PROIONTON TILIATRIKIS MONOPROSOPIKI ETAIRIA PERIORISMENIS EYTHINIS	**TMA**
6	ECLEXYS SAGL	**EXYS**
7	F6S NETWORK IRELAND LIMITED	**F6S**
7.1 (TP)	F6S NETWORK LIMITED	**F6S-UK**
8	PHARMECONS EASY ACCESS LTD	**PhE**
9	TERAGLOBUS LATVIA SIA	**TGLV**
10	NINETY ONE GMBH	**91**
11	EIT HEALTH GERMANY GMBH	**EIT**
12	UNIVERZITETNI KLINICNI CENTER MARIBOR	**UKCM**
13	SAN CAMILLO IRCCS SRL	**IRCCS**
14	SERVICIO MADRILENO DE SALUD	**SERMAS**
14.1 (TP)	FUNDACION PARA LA INVESTIGACION BIOMEDICA DEL HOSPITAL UNIVERSITARIO LA PAZ	**FIBHULP**
15	CENTRE HOSPITALIER UNIVERSITAIRE DE LIEGE	**CHUL**
16	PANEPISTIMIAKO GENIKO NOSOKOMEIO THESSALONIKIS AXEPA	**AHEPA**
17	VRIJE UNIVERSITEIT BRUSSEL	**VUB**
18	ARISTOTELIO PANEPISTIMIO THESSALONIKIS	**AUTH**
19	EIDGENOESSISCHE TECHNISCHE HOCHSCHULE ZUERICH	**ETHZ**
20	UNIVERZA V MARIBORU	**UM**

[2] CO: Coordinator. TP: linked third party.

Number[2]	Name	Short name
21	INSTITUTO TECNOLÓGICO DE CASTILLA Y LEON	**ITCL**
22	FUNDACION INTRAS	**INTRAS**
23	ASSOCIATION EUROPEAN FEDERATION FORMEDICAL INFORMATICS	**EFMI**
24	FEDERATION EUROPEENNE DES HOPITAUX ET DES SOINS DE SANTE	**HOPE**

1.2 Document Scope

This report, entitled D8.2 - SELP Compliance Report, documents the findings from T8.2 SELP Compliance framework. It describes: (1) the development of the appropriate SELP framework for assessing the SELP impact, and (2) how HosmartAI complies with that assessment.

D8.2 builds upon the previous deliverable, D8.1 - SELP Benchmark Report, which identified and documented ethical, legal, and social issues and regulatory framework relevant to HosmartAI. These identified SELP issues are the standards/goals to be met in the Project in terms of SELP context.

The central question of D8.2 is, what is the suggested Compliance Framework designed to address the identified issues, to assess the impact of the technologies involved, and to comply with the regulatory framework relevant to the Project, identified in the previous task/deliverable. To address the question, this report lays out the suggested framework, methodologies, and steps or processes of the Compliance Framework.

T8.2 SELP Compliance framework/D8.2 is distinguished from actual activity aiming to comply with the relevant regulatory frameworks and managing the protentional risks. In the forthcoming task 8.3 (T8.3) SELP Impact Assessment, an interactive questionnaire will be created, and two-way discussions between technical and legal/SELP teams will be initiated, which will be based on the findings of T8.2 and D8.2. Two of the major objectives of these processes are to identify: (1) the current status; and (2) the gap between current status and standards/goals to be met. The findings of the gap analysis will be documented as D8.3 SELP Impact Assessment. In a nutshell, the gap between “as-is” and “to-be” indicates the risks that needs to be managed/mitigated within the Project.

1.3 Document Structure

This document is comprised of the following chapters:

Chapter 1 presents an introduction to the project and the document.

Chapter 2 presents an overview of the SELP Compliance Framework and Impact Assessment, and provides an overview of how T8.2 SELP Compliance framework/HosmartAI_D8.2 SELP Compliance Report and T8.3 SELP Impact Assessment/D8.3 SELP Impact Assessment are related and interact.

Chapter 3 elaborates the standards or goals to be met from the SELP perspective.

Chapter 4 elaborates the processes and steps for the SELP Impact Assessment.

2 Overview of the SELP Compliance Framework and Impact Assessment

This section explains the overview SELP Compliance Framework and Impact Assessment as well as how each of the tasks and deliverables is related to each other.

D8.1 SELP Benchmark Report identified and documented ethical, legal, and social issues, as well as regulatory framework relevant to HosmartAI. In nutshell, the identified SELP issues are the standards/goals to be met in the Project in terms of the SELP context. For example, if Article 25 of the GDPR requires that "the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default," it is the standard that all data controllers of the Project need to meet.

This deliverable D8.2 - SELP Compliance Report focuses on the suggested Compliance Framework which is designed to address the identified issues, to assess the impact of the technologies involved, and to comply with the regulatory framework relevant to the Project ("Compliance Framework"). More specifically, D8.2 will lay out the suggested framework, methodologies, and steps or processes of the Compliance Framework. In a nutshell, the suggested Compliance Framework is a blueprint for the Project to assess the impact and to comply with the applicable regulatory and ethical frameworks.

In the forthcoming task T8.3 - SELP Impact Assessment, an interactive questionnaire based on T8.2 - SELP Compliance framework will be created, and two-way discussions between technical and legal/SELP teams will be initiated, based on the suggested Compliance Framework. Two of the major objectives of these processes are to identify: (1) current status (often referred to as "as-is" in practice); and (2) the gap between current status ("as-is") and standards/goals to be met (also referred to as "to-be" in practice). This process is sometimes referred to as "gap analysis" in practice. The findings of the gap analysis based on responses to the questionnaires and two-way discussions will be documented as D8.3 - SELP Impact Assessment. In nutshell, the gap between "as-is" and "to-be" indicates the risks that need to be managed/mitigated within the Project.

The following example helps illustrate what we have laid out above. Suppose an entity within the Project intends to use new technologies to process personal data, and taking into account the nature, scope, context, and the purposes of the processing, it is very likely that the processing would result in a high risk to the rights and freedoms of natural persons. Applicable law, Article 35 of the GDPR, requires data controllers to carry out an impact assessment that envisages processing operations on the protection of personal data. This is a standard or "to-be" that entities within the Project need to meet.

Responses to the questionnaire indicate the current status, or "as-is," of an entity. A particular entity may be aware and prepared to conduct an impact assessment; similarly, a particular entity may not be prepared and/or aware of the impact assessment required by the applicable law. The latter scenario indicates there's a gap between "as-is" and "to-be." If there's a gap between the two, it is the risk that needs to be addressed/managed.

D8.2 also covers the SELP requirements and elaborates the standards to be met or the "to-be" of the Project. It lays out how the SELP Requirements will be determined, including some methodologies/mindsets/principles that need to be considered or borne in mind. Also, it touches upon the classification of the SELP Requirements, which is designed to prioritise the requirements to make them effective and efficient.

Finally, D8.2 also covers the processes for the SELP Impact Assessment Framework. Specifically, it explains the HosmartAI model/cycle as well as 7 (seven) building blocks for SELP Impact Assessment.

3 The SELP Requirements

3.1 Introduction

SELP Requirements are the standards/goals, or the "to-be," that the Project aims to meet[3]. An important question to ask is, how and when will the SELP Requirements be decided, which we discuss below.

First, the SELP Requirements will be chosen and decided based on T8.1 Benchmark Report of the relevant regulatory and ethical frameworks and its deliverable D8.1 SELP Benchmark Report at the early stage of T8.3 SELP Impact Assessment. In other words, they will be the distilled version of the identified ethical, legal, and social issues and the relevant regulatory and ethical frameworks relevant to the Project. Further in T8.3 SELP Impact Assessment, the compliance questionnaires that will be created will be based on the SELP Requirements.

Second, they are not merely a transcription of the legal requirements. Requirements are rather re-written considering the operational aspect of compliance. For example, if the applicable law says "personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed," the Requirement may require "controller must have means that identifies whether or not personal data is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed." This is contrasted with a similar requirement which may state that "personal data to be processed is adequate, relevant and limited to what is necessary in relation to the purposes …" However, the latter tends to assume that the determination is only done at the initial stage. The reality is, determination must be done anytime there's a change in any relevant circumstances, which means a data controller must have the means/process to meet and operationalize such Requirement.

Third, there is a question as to how granular, or specific, these SELP Requirements should be. For example, the GDPR provides rights of the data subject, and generally, data controllers are obligated to comply with the rights when exercised. The specific Requirement may simply state "the exercise of the rights of the data subjects MUST be ensured," or alternatively, it can elaborate each right (e.g., right to access, rectification, erasure, etc.) corresponding to each SELP Requirement. While one cannot simply say either way is better than the other, the SELP Requirements would be made respecting and considering the principle of practicality/feasibility, supra, and taking the view that too long list of SELP Requirements would be detriment in terms of practicality/feasibility.

Finally, and importantly, there are some premises and/or (rebuttable) assumptions when choosing and deciding the SELP Requirements. Of these premises/assumptions, one is that the entity in the Project has some level of practical experience complying with some of the regulatory frameworks (e.g., GDPR, EU Medical Devices Regulation, and the like). This does

[3] For example, if Article 25 of the GDPR requires that "the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default," it is the standard that all data controllers of the Project need to meet.

not mean it decisively presumes that the entities are in compliance with the relevant regulations. Instead, it assumes the entities have some basic knowledge and practical experiences complying with applicable regulations they have been practicing. These premises/assumptions are necessary and acceptable because it enables to focus on the SELP issues that are unique, important, and novel to the HosmartAI and that require particular attention for the Project. Had the SELP Requirement covered the entire compliance issues including some that are too obvious for technical partners which have been practicing in their sector/domain/area, it would be detrimental to the technical partners and the SELP activity would be ineffective and inefficient.

3.2 Classification of the SELP Requirements: The MoSCoW Method

A question to ask is how much are the SELP Requirements required to be met because some of the SELP Requirements stem from legal requirements, while some others are listed as an aspirational Requirement partly because they may not be legal requirements, but stem from a best practice, for example.

The short answer is, not all Requirements are equally required. Some of them are more required than others, and some are required less than others. This means there should be prioritisation among the Requirements, and prioritising is often challenging. Particularly, when it comes to the implementation of new ideas and/or technologies, everyone in an organisation always wants everything to be done right away, but that is often practically impossible.

There are several tools available to make prioritisation easier, and the MoSCoW method is one of them. Being outcome-focused, the method provides a clear and measurable set of specifications, which can, over time, be continually monitored for compliance. The method labels each specific requirement, making it easier to prioritise. Even though the origin of this prioritization method is in software development, it is also highly applicable for market launches, product launches, starting a new business, or change processes. With MoSCoW Method, requirements are determined for the result of the project or product. The MoSCoW Method is about setting requirements by order of priority. The most important requirements need to be met first for a greater chance of success[4].

[4] VUB/LSTS has used MoSCoW method in multiple projects in the past, and suggests to use it in HosrmartAI. However, as there are multiple prioritisation tools or methodologies, which tool to be used will be discussed at the beginning stage of Task 8.3 (T8.3 SELP Impact Assessment) while considering relevant factors, including preference of partners.

The MoSCoW Method is an acronym made up of the first letters. The two Os have been added to make the word 'moscow' readable; they don't have any meaning themselves. The M stands for 'Must haves', S for 'Should haves', C for 'Could haves', and W for 'Won't haves' or 'Would haves'.

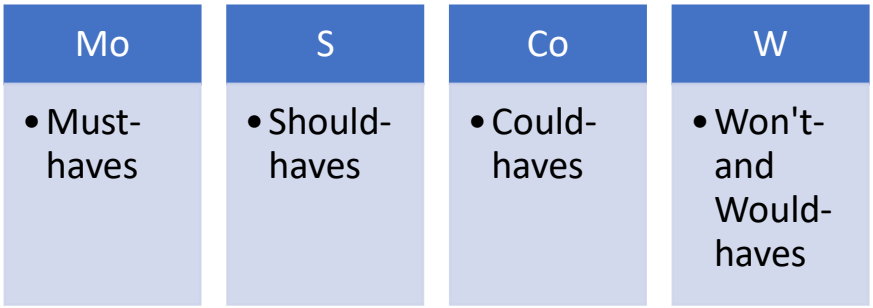


Figure 1: MoSCoW method

3.2.1 Requirements

It's a good idea to first specify the requirements before starting the MoSCoW Method. When determining the requirements, you should take into account what is important to the Project's stakeholders. Brainstorming with everyone involved will lead to good, qualitative requirements. The requirements are prioritised to prevent them from becoming too expensive or unrealistic. The main goal is to come up with requirements that add the most value for the consortium. The project requirements are divided into one of the following categories:

3.2.2 M - Must haves

These are about the minimal requirements that are determined in advance that the end-result has to meet. Without meeting these requirements, the project fails and the product won't be use-able. They are necessary for a workable product and there is no alternative. The 'Must haves' are essential. MUST is also explained as an acronym that stands for **M**inimum **U**se-able **S**ubse**T**s.

3.2.3 S - Should haves

These are additional and much desired requirements that have a high priority, but are not essential for a usable end product. The product will be usable even if these requirements aren't met. When they are met, they will only add to the value of the product. Depending on the available time, you can always return to these requirements at a later time.

3.2.4 C - Could haves

These requirements can be considered if there's time left. If not, it's no problem and will not have a negative effect on the final result. The 'Could haves' have a lower priority than the 'Should haves'. This option will only be included if there really is more than enough time to make it work. This category is also referred to as 'nice to have'; they're more a wish than an absolute requirement.

3.2.5 W - Won't haves (and would haves)

These are about wishes for the future that is often impossible to realise or cost a lot of time. If it is simply not possible, it's best not to waste any energy on it. If it is achievable, then a lot of time (and money) will have to be invested and it's labelled a 'Would have'. 'Would haves' are often followed upon at a later stage after the initial project is finished.

3.3 Overview of the SELP Requirements

The previous deliverable 8.1, entitled D8.1 SELP Benchmark Report, has identified ethical, legal, and social issues as well as the regulatory framework relevant to HosmartAI. In sum, they concern:

- Various legal framework on fundamental rights/human rights;
- Patients' rights under the EU Patients' Rights Directive;
- Various legal frameworks on data protection/privacy law, namely the GDPR;
- Various ethical and social issues, such as "black box effect," discrimination, and unfairness as well as concepts such as explainable AI; and
- EU Medical Devices Regulation

These SELP issues and frameworks will become more manageable and achievable once they are converted into specific SELP Requirements. The table below shows some of the examples of SELP Requirements.

Table 2: Examples of SELP Requirements.

SELP ID	Reference (Chapter in D8.2)	Standard (condition/goal) to be met	Classification
1.	. . .	. . .	. . .
. . .	. . .	. . .	. . .
3	. . .	Data subjects MUST be informed about the intended data processing operation during the duration of HosmartAI.	MUST
4	. . .	The legal ground and the purpose of the data processing MUST be defined.	MUST
5	. . .	If the processing of personal data will be based on the consent of the data subject, it MUST be informed, specific and freely given.	MUST
6	. . .	The end date of the processing SHOULD be determined, and it SHOULD be made clear, what will happen with the personal data afterwards.	SHOULD
7	. . .	The security of data MUST be ensured	MUST
8	. . .	The rules of access to personal data (with special attention to its conditions, mode, and limits) MUST be clearly defined	MUST
9	. . .	The processing operations MUST be documented.	MUST
10	. . .	The exercise of the rights of the data subjects MUST be ensured.	MUST
11	. . .	Information SHOULD be provided to the data subject about the processing operation within HosmartAI.	MUST
12	. . .	Unused personal data SHOULD be deleted automatically.	SHOULD
13	. . .	The processed data MUST be relevant and accurate for the purposes of data processing. The HosmartAI system should record and work with only those types of data which are necessary to reach the goal of the processing.	MUST
14	. . .	The processing of personal data MUST be based on a legitimate legal ground and shall have specified purposes	MUST
15	. . .	Appropriate technical and organisational measures MUST be applied to ensure a level of security appropriate to the potential risk.	MUST
. . .	. . .	. . .	. . .
N	N.N.N.N	. . .	. . .

4 Processes for the SELP Impact Assessment Framework

4.1 Introduction

This section lays out the processes and steps for the SELP Impact Assessment Framework. The objective of the SELP Impact Assessment within the Project is to assess the implications of ethical, legal, and social issues, and to manage the risks associated with the issues. To do so, the Project will need to fill the "gap" between "as-is" and "to-be," as mentioned earlier. It is often tempting to achieve the best result, by attempting to: list and manage all the risks; treating all issues and risks equally and importantly as much as possible; accomplish maximum security by implementing all possible security measures; and in the first attempt. However, such an attempt is often: impossible, too costly, does not last long; and/or produces rules that are ignored.

In order to make changes from "as-is" "to-be," effectively and efficiently, it is essential that such activities must be on-going, continuous, and consecutive/successive.

In practice, one well known and generally accepted model to ensure such on-going and continuous activity is referred to as PDCA model/cycle. PDCA is an acronym of **P**lan, **D**o, **C**heck, and **A**ct, and it is well known as a four-step model to carry out a change. Plan is a step to recognize and determine the plan for a particular change. The 'Do' is a step to test and carry out the plan, often in smaller steps. Check is a step to review the results of the test/change and to analyse if the 'Do' step is going as planed in the Plan step. Some of the questions that can be asked in this step are:

- Was the plan appropriate?
- Is the change (implementation of the plan) in the Do step producing expected results?
- Has the change produced any unintended problems?

The 'Act' is a step to respond to the findings of the Check step. For example, it can be: modifying the plan because the plan does not bring expected results and/or produces unintended problems; or modifying how to implement the plan because the way how the plan was implemented did not produce the expected result and/or produced unintended problem.

For HosmartAI project, we suggest a more detailed and tailored model/cycle, which has been used by VUB/LSTS in many other projects in the past [REF-01][REF-02][REF-03]. The model consists of 7 steps/processes, or "building blocks." They are: (1) Threshold analysis; (2) Initiation of the assessment; (3) Identification, characterisation, and description of the systems; (4) Assessment; (5) Stakeholder consultation; (6) Risk management plan; (7) Monitoring and reviewing[5]. In the following sections, each of the "building blocks" are explained in detail.

[5] In the past, VUB/LSTS conducted impact assessment in using the same methodology consisting of 8 steps or 5 steps, but the essence remains the same.

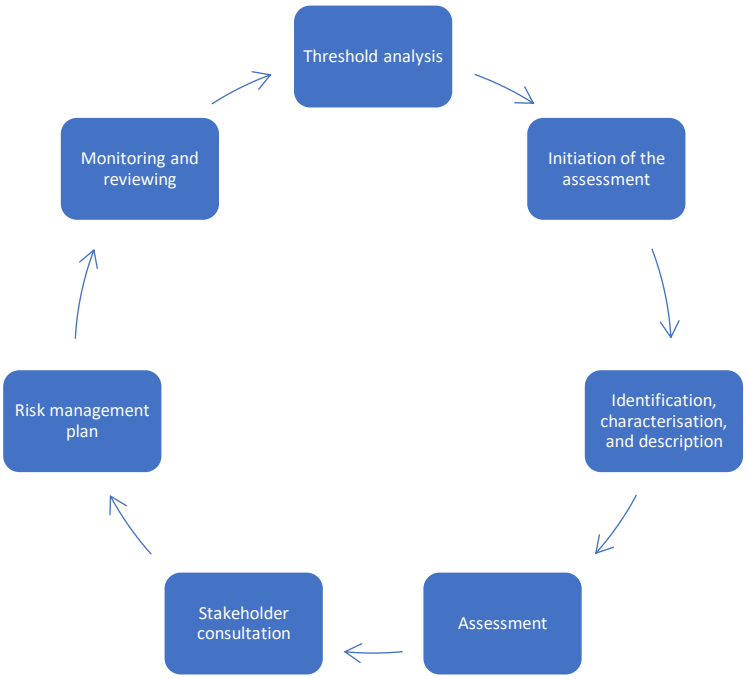


Figure 2: HosmartAI model/cycle

4.2 Threshold analysis (screening)

The first step of the SELP framework is a threshold analysis. This step determines whether the process of impact assessment is warranted or necessary for a planned initiative or a set of similar initiatives, in a given context [REF-01]. This step also includes scoping, which, inter alia, identifies societal concerns, ethical issues, and corresponding legal as well as other regulatory requirements.

An impact assessment, beginning with a threshold analysis, shall be carried out at an "early stage." For example, in the data protection/privacy domain, the number of GDPR provisions as well as recitals imply or explicitly require IA should be carried out prior to the processing. Article 35(1) and Recital 90 explicitly state that "the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations."[6] Article 25 assumes that "at the time of the determination of the means for processing" the risks are already known, and that "ideally, full and detailed consideration of privacy issues should precede system design."[7] Furthermore, Recital 89 implies similarly.

The purpose of threshold analysis is to determine whether or not impact assessment ("IA") is necessary. There are several reasons why an IA process should be initiated. They include, for example: (1) ethics/legal/social acceptance specifying situations in which there is an obligation to carry out an IA; (2) appreciation by an organisation that a proposal has broad

[6] Article 30 and Recital 90.
[7] Article 25 GDPR.

and significant implications that should be subjected to an impact assessment; (3) public concerns; and the like. This step includes the following elements:

- Determining the scope of the impact assessment
- Pre-assessment of the need to conduct an impact assessment
- Selection of criteria, e.g., on which the pre-assessment is conducted, e.g., impacts on rights and freedoms, impacts on social norms, impacts on information security, impacts on market, motivations and timing, legal basis and public concerns

4.3 Initiation of the assessment

Once it is decided that an impact assessment is necessary, the responsible person (e.g., the task leader or other decision-maker) will determine the roles and responsibilities of the team, which conducts the impact assessment.

A team comprising of experts might be deemed necessary in order to be able to carry out the impact assessment effectively. The designated team, along with those who set the direction of the application or technology development, will determine the grounds of the work, such as communication platforms to be used, timing, involved persons, and the like. Furthermore, the determination of the grounds against which the impact assessment is to be conducted should be further clarified. The role of this step within the aforementioned context is to outline in broad terms the relevant societal concerns. These requirements will be used to create an "impact framework" which will have to be taken into consideration and adhered to in the Project. These requirements will be clarified with the other partners through a questionnaire, which will be subsequently used to produce the report on the D8.3 SELP Impact Assessment. This step includes the following elements:

- Designation of the IA team
- Defining the resources needed
- Setting the determining grounds - SELP requirements.

4.4 Identification, characterisation, and description of the systems

A project leader may not always have the expertise on SELP Requirements. Thus, cooperation with experts in SELP, such as lawyers, is essential. Strong and organic cooperation, in terms of effective and regular communication between the parties, exchange of information between the parties (project partners and IA team) is of paramount importance, especially where high-end technology is applied (e.g., artificial intelligence, robotics, and the like).

To achieve strong and organic cooperation, on the one hand, the project partners shall describe extensively the details and functioning of the project; on the other hand, the IA team shall describe the reasoning behind the whole assessment, including its goals, length, stages, intermediate and final results, liabilities and possible consequences. Issues can also arise from the different goals and professional language the parties use. The meaning and importance of the SELP requirements might be self-evident for the IA team, but entirely confusing for other project partners, and vice-versa. The parties need patience, openness, and the intention to understand the points of view of the other parties. There are numerous, developed tools

for the parties which help to understand the main goals of the procedure, e.g., charts or questionnaires. Also, detailed questionnaires will be used to identify the potential risks of the project. This step includes identification of the following elements:

- The use case;
- Records of processing activities[8];
- System information, including information transfer;
- Description of primary and supporting assets of the system, including identification and prioritization of assets;
- Internal and external stakeholders.

4.5 Assessment

As anticipated above, the risk itself is the core element and subject of a risk/impact assessment. Risk can have an impact either on an individual, group or society. The rationale behind the assessment is mitigating or avoiding adverse consequences of these risks prior to their occurrence. The assessment of risks stands on three pillars: identification, analysis and evaluation. First, the source of risk, the risk itself and its outcomes should be identified precisely. In the analysis phase, the identified risk is understood by measuring the likelihood of its occurrence and, more importantly, the severity of the possible consequences. Afterward, the results of the analysis are evaluated according to the relevant classification in which each risk is associated with its' relevant severity level. This will enable to single out the elements of the system in need of interventions designed to minimize or avoid the adverse consequences. This step includes the following elements:

- Identification of relevant risks, including threats and vulnerabilities;
- Analysis of feared events;
    - Impact of events
    - Likelihood of threats
- Evaluation of feared events.

4.6 Stakeholder consultation

The rationale behind stakeholder consultation is to provide insight about the identified and analysed risks as seen from the point of view of those actors affected by the application or service. If the impact assessment is conducted from a single viewpoint, risks and their impacts might be overlooked. A consultation with stakeholders can ameliorate the analysis of the risks, impacts, and mitigating measures by involving internal (partners in the Project) and external (the affected public, business, community, environment, etc.) stakeholders. If the stakeholder engagement is conducted properly, it will provide the HosmartAI system with a competitive advantage in terms of increased transparency, trust, such as by providing assurance of the outcome of the risk management; better collection of risk information; increased mutual understanding among decision-makers and stakeholders; better

[8] Art. 30 GDPR.

communication of the results of the assessment; improved awareness; etc. This step includes incorporation of the consultation in the assessment report.

4.7 Risk management plan

When the risks are sufficiently evaluated the impact assessment identifies appropriate and effective responses and mitigation techniques in forms of recommendations to project partners. If the project/task leader intends to address the risks, the most practical form of treatment should be selected. During the selection of the appropriate mitigating measures, the decision-maker should take into consideration all the SELP Requirements equally. At this stage, the decision-maker must make clear which risks are residual and accepted/acceptable. Finally, during the risk treatment step, the decision-maker will bear in mind that, failing to address the identified risks may result in social, economic, or reputational damages. This step includes the following elements:

- Analysis of controls and measures in place or planned;
- Determination of the probability of an incident;
- Assessment of the potential impact of a threat;
- Priority classification of risks;
- Recommendations for controls and measures;
- Documentation of results (mandatory with GDPR).

4.8 Monitoring and reviewing

Review and/or audits are critical to ensure that the impact assessment is, first, carried out properly and, second, that its recommendations are sufficiently implemented. Review and/or audits are indispensable, as project leaders might initially state that they accept and would implement the suggested mitigation measures, but in reality, they might fail to implement them. Thus, the implementation of the recommendations should be monitored and periodic reviews should be conducted with supporting documentation. If the project changes in a significant way resulting to affect the impact on SELP Requirements, depending on the magnitude of the changes, the impact assessment should be revised (wholly or partially) and carried out again. In HosmartAI, the first monitoring report, D8.4 SELP Continuous Monitoring Report 1 will be delivered in Month 25 and the second monitoring report, D8.5 SELP Continuous Monitoring Report 2 in M41. This step includes the following elements:

- Periodic monitoring and review;
- Flexibility of IA in case scenarios change.

5 References

[REF-01]	Dariusz Kloza et al., Data protection impact assessment in the European Union: developing a template for a report from the assessment process (2020), https://osf.io/preprints/lawarxiv/7qrfp/.
[REF-02]	Dariusz Kloza et al., Towards a method for data protection impact assessment: Making sense of GDPR requirements (2020), https://osf.io/es8bm.
[REF-03]	Dariusz Kloza et al., Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals (2020), https://osf.io/b68em.