SHAPES

Smart and **H**ealthy **A**geing
through **P**eople **E**ngaging in supportive **S**ystems

D8.10 – Privacy and Ethical Risk Assessment

Project Title	Smart and Healthy Ageing through People Engaging in Supportive Systems
Acronym	SHAPES
Grant Number	857159
Type of instrument	Innovation Action
Topic	DT-TDS-01-2019
Starting date	01/11/2019
Duration	48

Work package	WP8 – SHAPES Legal, Ethics, Privacy and Fundamental Rights Protection
Lead author	Harri Haapaniemi (LAUREA)
Contributors	Sari Sarlio-Siintola (LAUREA), Katja Tikkanen (LAUREA), Jyri Rajamäki (LAUREA), Jaakko Tyni (LAUREA), Marjo Valjakka (LAUREA), Rauno Pirinen (LAUREA)
Peer reviewers	Ioannis Kefaloukos (HMU); Evangelos K. Markakis (HMU); Marta Sýkorová (UP)
Version	V1.0
Due date	30/06/2023
Submission date	28/06/2023
Dissemination Level	PU Public

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

Revision History

Table 1 Revision History

Revision #	Date	Editor	Comments
0.1	06.03.2023	Harri Haapaniemi,	Created
0.2	07.03.2023	Sari Sarlio-Siintola	ToC
0.3	28.04.2023	Harri Haapaniemi	ToC, Content
0.4	09.05.2023	Harri Haapaniemi: Marjo Valjakka	Content check
0.5	23.05.2023	Sari Sarlio-Siintola	Chapter 6 and 7
0.7	25.5.2023	Marjo Valjakka, Rauno Pirinen, Harri Haapaniemi, Jyri Rajamäki, Jaakko Tyni	Chapter 1, Chapter 2, Chapter 3, Chapter 4, Chapter 5, Chapter6, Chapter 7
0.8	31.5.2023	Harri Haapaniemi	Chapter 1, 2,3 ,4, 5
0.9	01.06.2023	Harri Haapaniemi, Sari Sarlio-Siintola	All chapters
0.91	05.06.2023	Harri Haapaniemi, Sari Sarlio-Siintola, Katja Tikkanen, Jyri Rajamäki	All chapters
0.92	06.06.2023	Harri Haapaniemi. Sari Sarlio-Siintola, Katja Tikkanen	All chapters
0.93	13.06.2023	Harri Haapaniemi. Sari Sarlio-Siintola, Katja Tikkanen	All chapters
1.0	26.06.2023	Harri Haapaniemi, Sari Sarlio-Siintola	All chapters

Table of Contributors

Table 2 Deliverable Contributors

Section	Author(s)
Table of Contents	Harri Haapaniemi, Sari Sarlio-Siintola
Chapter 1	Sari Sarlio-Siintola, Harri Haapaniemi
Chapter 2	Marjo Valjakka
Chapter 3	Katja Tikkanen, Harri Haapaniemi
Chapter 4	Jaakko Tyni, Jyri Rajamäki
Chapter 5	Sari Sarlio-Siintola
Chapter 6	Rauno Pirinen, Jyri Rajamäki
Chapter 7	Sari Sarlio-Siintola, Harri Haapaniemi

Table of Acronyms and Abbreviations

Table 3 Acronyms and Abbreviations

Acronym	Full Term
AI	Artificial intelligence
CFR	Charter of Fundamental Rights
CJEU	Court of Justice of the European Union
CRPD	United Nations Convention on the Rights of Persons with Disabilities
CSR	Corporate Social Responsibility
DMP	Data Management Plan
DPIA	Data Protection Impact Assessment
GDPR	General Data Protection Regulation
H&C	Health and Care
HLGE	High-Level Expert Group on Artificial Intelligence
HMI	Human-machine interaction
IA	Innovation Action
ICT	Information and communication technology
IoT	Internet of things
IT	Information technology
OSE	European Social Observatory
SA	Situational awareness
SME	Small and medium size enterprises
SPC-WG-AGE	Social Protection Committee Working Group on Ageing
TEU	Treaty on European Union

Keywords

Risk management, ethics, ethical requirements, fundamental rights, values and norms, ethical guidelines, privacy and data protection, cybersecurity, mitigation

Disclaimer

This document contains information which is proprietary to the SHAPES consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or parts, except with the prior written consent of the SHAPES coordinator.

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

List of Figures

List of Tables

Executive Summary

This deliverable, the second SHAPES Privacy and Ethics Risk Management Assessment (D8.10), presents the results of the privacy and ethical risk assessment in the SHAPES project. The focus of the risk work has been on risks identified by the pilots during the second half of the project. In addition to this, risks identified earlier in the first half of the project (D8.9) and further investigated during this second half are included in the analysis in order to provide a comprehensive picture of the risks that are relevant to the SHAPES solution, including both technology, user processes and governance/business models. This way the deliverable also better serves the work to be performed under WP3 regarding the SHAPES governance model in the future, including privacy and ethics risks related activities.

The risk data collection was carried out using multiple methods and tools involving various stakeholders. Both a top-down and bottom-up approach was applied. If there is a possibility of a negative impact, these possibilities are treated as risks. If the outcome is more positive, it is identified as an opportunity. The ethics risks identified are mapped against the ethical requirements outlined in D8.14. Minor updates were made to the ethical requirements, including a few new requirements (see Appendix 1).

The SHAPES risk work has revealed that the essential part of the risks concern privacy and data protection, and other data related risks. In addition, risks and opportunities related to access to fair and sustainable services as well as to growing inequality, dehumanisation of care, and independence and autonomy of end users raised concern. Generally speaking, most of the risks are manageable as long as the ethical requirements (see Code of Conducts in the D3.6 SHAPES Governance Model) are acknowledged and followed.

The purpose of this deliverable and ethics risk management is to ensure that the SHAPES initiative becomes an ethically responsible endeavour and a positive innovation for its various end users and service providers, as well as for society as a whole.

1 Introduction

1.1 Rationale and purpose of the deliverable

This deliverable D8.10: SHAPES Privacy and Ethical Risk Assessment (PU, Report, LAUREA, M42) continues work started by D8.9 and provides a comprehensive *privacy and ethical risk assessment* of the SHAPES Integrated Care Platform and Digital Solutions.

This second SHAPES ethics and privacy risk management deliverable (D8.10) is mainly composed of inputs coming from pilots' ethics risk workshops, AI assessments, and DPIAs (Data Protection Impact Assessment) during the second half of the SHAPES project. In addition to this, risks identified earlier in the first half of the project (D8.9) and further investigated during this second half are included in the analysis in order to provide a comprehensive picture of the risks that are relevant to the SHAPES solution, including both technology, user processes, and governance/business models.

1.2 Task 8.4: Privacy and Ethical Risk Assessment for the SHAPES Platform

Task 8.4 implements a comprehensive privacy and ethical risk assessment to mitigate potential unintended impacts of the SHAPES Platform on privacy and other fundamental rights as well as ethical values. It will also establish mitigation strategies and actions to avoid any adverse effects. Throughout the project, identified issues and the results of the assessment were discussed and explained in project meetings. Figure 1 describes the overall process of the provision of this deliverable.

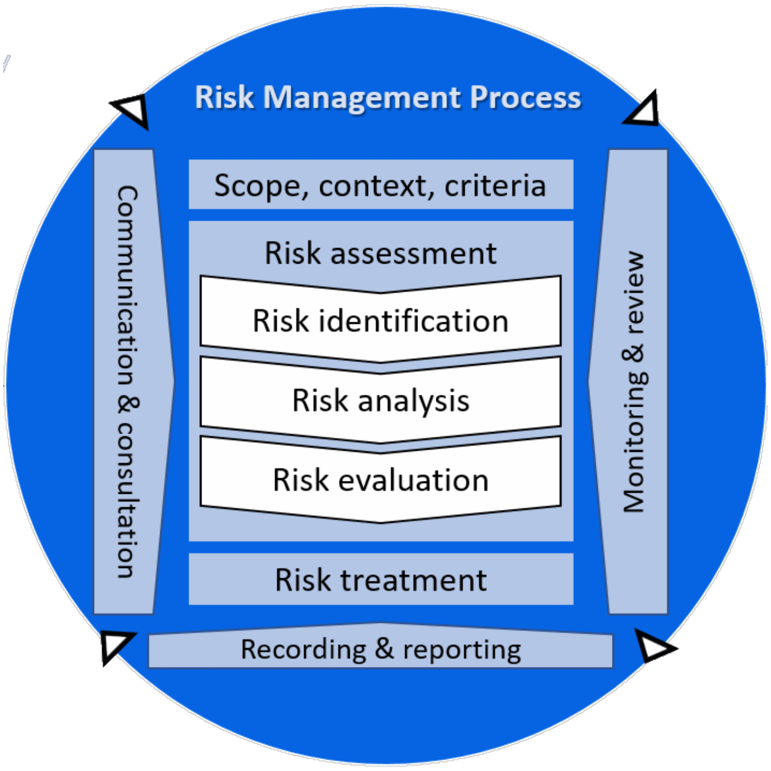


Figure 1 The risk management process (adopted from D8.9)

The risk management process and methodology were described in full in deliverable 8.9. but in essence, the SHAPES ethics and privacy risk management process is based on the following five steps: 1) identify the risk, 2) analyse the risk, 3) evaluate the risk, 4) risk mitigation, and 5) follow up.

During the second half of SHAPES T8.4, various tools and partners were used in order to finalise D8.10. See Figure 2 below.

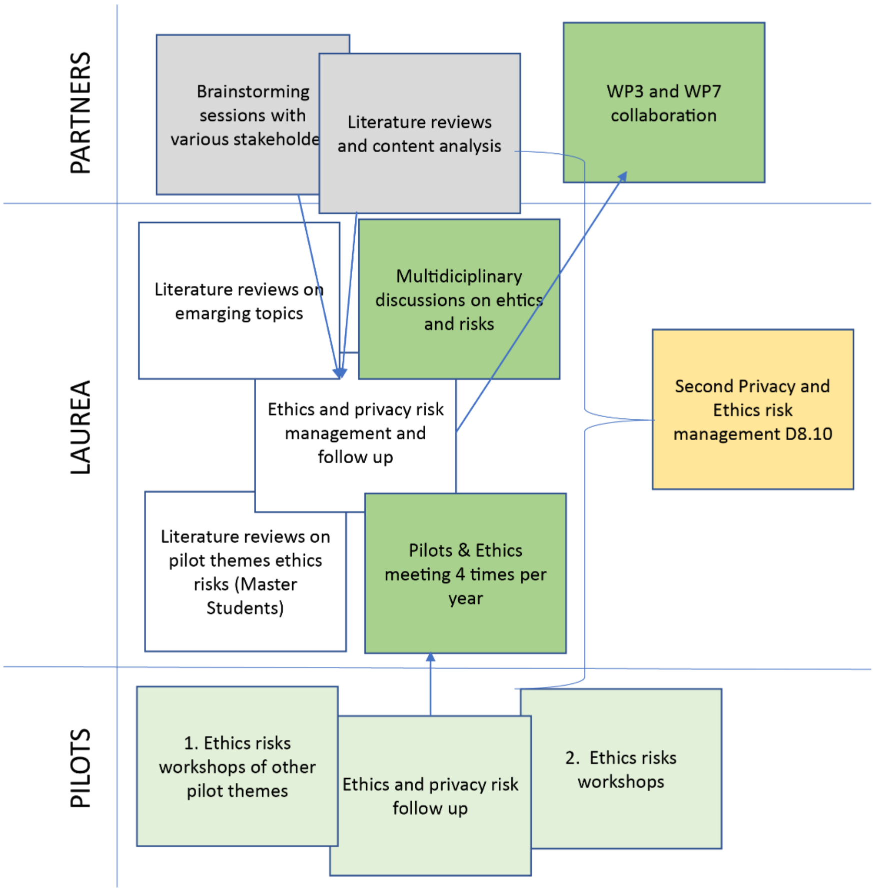

PARTNERS
LAUREA
PILOTS
Brainstorming sessions with various stakeholde
Literature reviews and content analysis
WP3 and WP7 collaboration
Literature reviews on emarging topics
Multidiciplinary discussions on ehtics and risks
Second Privacy and Ethics risk management D8.10
Ethics and privacy risk management and follow up
Literature reviews on pilot themes ethics risks (Master Students)
Pilots & Ethics meeting 4 times per year
1. Ethics risks workshops of other pilot themes
Ethics and privacy risk follow up
2. Ethics risks workshops

Figure 2 Activities planned for the second half of the SHAPES platform

In Figure 3, the Ethics Governance model in SHAPES is explained.

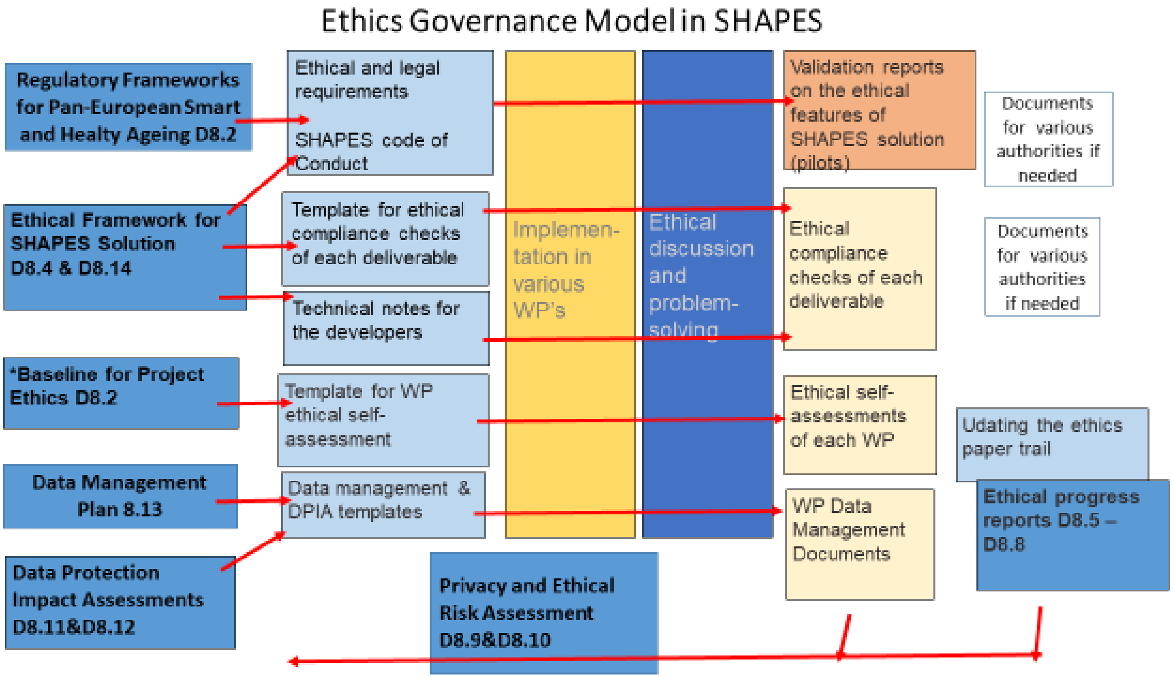

Ethics Governance Model in SHAPES
Regulatory Frameworks for Pan-European Smart and Healty Ageing D8.2
Ethical Framework for SHAPES Solution D8.4 & D8.14
*Baseline for Project Ethics D8.2
Data Management Plan 8.13
Data Protection Impact Assessments D8.11&D8.12
Ethical and legal requirements
SHAPES code of Conduct
Template for ethical compliance checks of each deliverable
Technical notes for the developers
Template for WP ethical self-assessment
Data management & DPIA templates
Implemen-tation in various WP's
Ethical discussion and problem-solving
Validation reports on the ethical features of SHAPES solution (pilots)
Ethical compliance checks of each deliverable
Ethical self-assessments of each WP
WP Data Management Documents
Documents for various authorities if needed
Documents for various authorities if needed
Udating the ethics paper trail
Ethical progress reports D8.5 – D8.8
Privacy and Ethical Risk Assessment D8.9&D8.10

Figure 3 SHAPES Ethics Governance Model (adopted from D8.2)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

1.3 Key inputs and outputs

Key inputs

The content of this deliverable is composed mainly of the following inputs:

- D8.14 The SHAPES Ethics Framework, which identifies key challenges of digitalization in the context of older persons' wellbeing and defines the ethical requirements that have provided the backbone for much of the work done in T8.4, including this deliverable.
- D8.9 the first SHAPES Privacy and Ethics Risk assessment the contents of which have been further combined with the new risks identified during this second half of the project.
- Risks and mitigation activities, which have been defined as outputs of SHAPES pilots' Privacy and data protection Impact Assessments (DPIAs).
- Materials that have been collected from the workshops of seven different pilots and their expert networks. The workshops were organized by Laurea and SHAPES pilots, and they were carried out between June 2022 and January 2023. The experts considered various ethical risks, especially from the point of view of EU fundamental rights, bioethics, Ethics of Care, Human Capabilities, and GPDR.
- ALTAI questionnaires, which have been filled in by pilots utilizing Artificial Intelligence solutions.
- The ethics advisory board (EAB). The EAB has had four meetings during the project. Discussions on privacy and ethical risks have been an essential part of each meeting.

Key outputs

The idea of this deliverable's outputs is to provide inputs for the design of the final SHAPES solution and its governance and business models as part of the work of WP3 and WP7. In addition, ISO 25553 work as part of WP2 will be informed on these ethical? risks outcomes. These include the following deliverables:

- D.2.3: Cultivating Age-Friendliness (see Code of Conduct for multigenerational neighbourhoods)
- D3.6: SHAPES Collaborative Governance Model (see Codes of Conducts for SHAPES technical platform, SHAPES socio-technical platform, and SHAPES network)
- D3.10: SHAPES Change Management and Implementation Handbook
- D3.11: SHAPES Recommendations
- D7.2: SHAPES Socio-Economic Sustainability
- D7.3: SHAPES Business Plan

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

Outputs of this ethics risk work will be also disseminated in conferences, including e.g., the eHealth2023 conference in Finland in October 2023.

1.4 Structure of the document

After the introduction and presentation of the deliverable in Chapter 1, Chapters 2, 3, and 4 are based on pilot activities during the last half of the SHAPES project.

Chapter 2 provides a description of how privacy and data protection risks have been taken into consideration in SHAPES as part of the pilots' DPIA process.

In Chapter 3 we review the main risks identified among the pilots from the viewpoint of EU fundamental rights, the UN convention on the Rights of Persons with Disabilities, Bioethics, Ethics of Care, and Human Capabilities.

In Chapter 4 we describe the risks related to the use of artificial intelligence including the risk identification and mitigation process.

Chapter 5 shows the results of the ethics advisory board meetings and discussions on governance and business models which are relevant from the viewpoint of risks and opportunities.

Chapter 6 contains other central topics related to risk management discussed partly earlier in D8.9, including data management and cyber security.

Chapter 7 provides a conclusion for the deliverable.

2 Privacy and data protection risks

This chapter describes how privacy and data protection has been taken into consideration in SHAPES. The main focus of this chapter is on the SHAPES project, but the same principles will apply also in future SHAPES services. The principles described in this chapter were implemented in SHAPES processes and different digital solutions. The practical implementation of privacy and data protection principles was assessed as part of the DPIAs that were to be done for the pilots and also for the SHAPES platform. The SHAPES ethical requirements complemented this chapter by giving more detailed descriptions for practical implementation. The aim was to describe what needs to be done and let all SHAPES partners who process personal data then decide how the implementation will be done.

The data management risks are updated in the data management plan D8.13. In D8.10, there are examples that build on the first SHAPES review process and explore the security and data management risks approach and increase the promotion of 1) a table of SHAPES DMP (Data Management Plan) risk assessment attributes, 2) a table of selected cases for multiple case study analysis increasing the understanding of risks in the appropriate research domain (SHAPES security and data governance domain), 3) a description of higher level categories of security and data management risks in SHAPES, 4) a description of higher level categories of security and data management risks in SHAPES, 5) a data risk mitigation table for co-creation of a SHAPES security and data management risk and mitigation foundation and 6) a table of the most relevant techniques and mechanisms that can be considered for mitigation of risks in a typical SHAPES security and data management system.

2.1 The risk identification and mitigation process

As part of the data protection impact assessments (DPIA), the pilots were advised to assess the context, necessity, and proportionality of data processing as well as data protection risks, their probability and impact, and proposed actions to mitigate the risks before the pilot. The DPIA process is described in the deliverable D8.11.

Despite **pilots and use cases** having **their** own processes and documentation, are data protection impact assessments (DPIA) an integral part of risk management. The difference is that the requirements come from the General Data Protection Regulation (GDPR) and the risks apply to individuals as data subjects. However, the risk to the data subject can also lead to operational risk and reputational damage. Above all, the process is designed to ensure data security, data protection and the rights of the data subjects throughout the data lifecycle.

As part of the DPIA, the pilots were advised to assess the context, necessity, and proportionality of the processing as well as the data protection risks, their probability

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

and impact, and the proposed actions to mitigate the risks. The DPIA process is described in deliverable D8.11.

The pilots were able to make use of the SHAPES' DPIA self-assessment risk framework, which included pre-assessed risks, but each use case also assessed the risks from its own perspective and added risks related to, for example, the device or application used in the use case.

As the risk assessments were carried out before starting the pilots, not all risks were necessarily covered in the beginning, such as the loss of control over future use of personal data. Therefore, the pilots were advised to follow up on the DPIA process and document possible new risks and actions as well as assess the adequacy of the planned actions during the use case.

Although the DPIA process with its documentation requirements can be found to be time-consuming, up to date DPIA documentation is important for ensuring data security and privacy during the project as well as for further development. The DPIA process also gave time to mitigate the risks found. The Data Manager of SHAPES went through all the DPIA documents in the spring of 2023 and ensured they were up to date. Due to the workload of the pilots, some reports were still incomplete, but follow-up of the risks have been ensured in other ways.

2.2 Identified risks

The use cases listed a total of nearly 60 different data protection risks. The most significant risks were prioritised, and they were related to cyber security, data integrity, and consent management. According to the pilots, the most significant risks were:

- Loss or unintended modification of data (listed in 16 use cases)
- Uses of data not contemplated regarding consent or incomplete consent (16 use cases)
- Cyber attack / Data breach (13 use cases)
- Software conflicts between user's devices and SHAPES technologies (7 use cases)

In addition to the above, use cases named risks with lower probability and/or impact. Although their risk significance was assessed as markable but not significant, their prevalence indicates that low-risk activities have also been taken into account. The most commonly mentioned risks are listed below:

- Keeping and using identifiable data longer than needed (listed in 19 use cases)
- Data is collected and stored unnecessarily (listed in 18 use cases)
- Identity revealed (listed in 13 use cases)
- Information collection might be seen as intrusive (12 use cases)

- Incorrect manual input of data (11 use cases)
- Collection of a wider set of information than individuals might expect (10 use cases)
- Missing data (10 use cases)
- Pseudonymized information becomes identifiable unintentionally (9 use cases)

2.3 Mitigation activities

Every use case had individual mitigation plans for both the significant and markable risks. Some actions were scheduled to be completed before the start of the pilot, such as agreeing on the processing of personal data and requirements for technical solutions. However, most of the actions had to be followed up throughout the pilot.

Table 4 shows a summary of the mitigation activities in the pilots, which will also provide pointers for future DPIA processes.

Table 4 Summary of mitigation activities

Topic	Mitigation activities	Whose responsibility to mitigate	Ethical requirements in D8.14 and other activities needed
Loss or unintended modification of data	Defining a process for a double human check validation process and ensure backup of systems.	Service providers	GE42, ET20, ET14
Uses of data not contemplated regarding consent or incomplete consent	Legal department to review the consent form and its possible updates.	SHAPES governance SHAPES network	New requirement added
Cyber attack / Data breach	Setting up monitoring systems and incidence reporting protocols. Upon incident detection, the incident response team will assess the event consequences towards designing and deploying the necessary technical and organisational control measures.	Service providers SHAPES governance SHAPES network	ME14, ET23, GE55, GE41
Software conflicts between user's devices and SHAPES technologies	Preparing the necessary updates where needed.	Service providers SHAPES network	ET5

Keeping and using identifiable data longer than needed	Setting up a data retention schedule which will be followed. If withdrawal of consent is notified, all data relating to that data subject will be identified using the data plan and erased. All data collected in the SHAPES pilot, including directly identifiable data and consent forms, will be deleted at the end of the SHAPES Project in October 2023.	SHAPES governance SHAPES network	
Data is collected and stored unnecessarily	Applying data minimisation. Selection of unobtrusive devices and digital solutions to gather data.	Service providers SHAPES governance	ET11
Identity revealed	Identifiable information stored securely and with limited access. Security breach events to be assessed with a focus designing and deploying the necessary control measures.	Service providers SHAPES governance	ET11
Information collection might be seen as intrusive	Careful and detailed explanation why the data is being collected and how the data minimisation has been applied. Updating the information sheet and privacy policy if necessary. Setting up a contact point for participant concerns.	SHAPES governance SHAPES network	GE23, PE4
Incorrect manual input of data	User training sessions. Prompt interventions if needed.	SHAPES network	PE 4

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

Collection of a wider set of information than individuals might expect	Applying data minimisation. Providing participants with detailed information about the conduct of the study before they agree to participate.	SHAPES governance SHAPES network	ET11, PE4
Missing data	Performing connectivity tests on a regular basis.	Service providers	(technical requirement)
Pseudonymized information becomes identifiable unintentionally	The participant list linking the pseudonymised ID to the individual will be destroyed and the identifiable data set will be deleted.	SHAPES governance SHAPES network	ET6

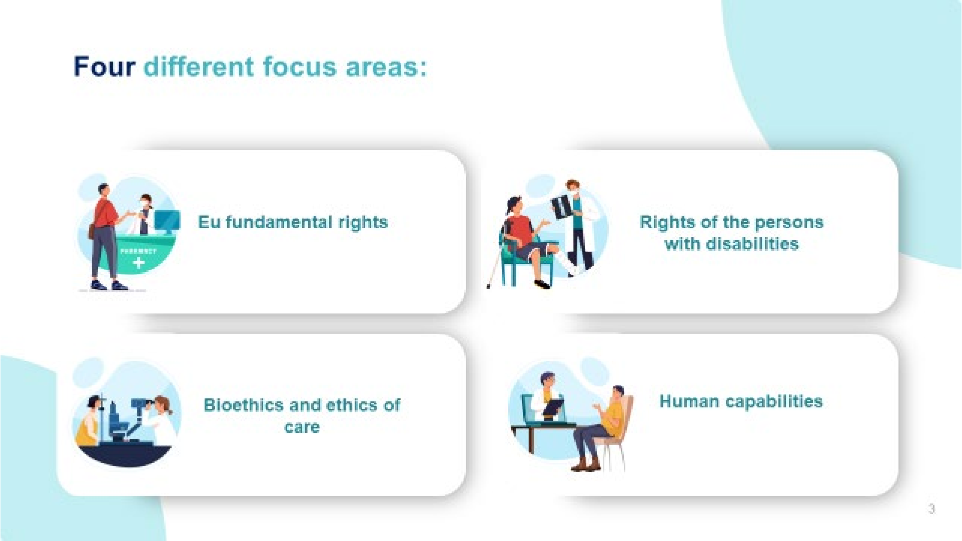
3 Risks related to central values, principles, and rights of end users

As mentioned in Chapter 2, the pilots conducted a DPIA (Data Protection Impact Assessment) including risk identification and a mitigation plan. However, in order to identify pilot related ethical risks beyond privacy and data protection, Laurea created an online workshop model for pilots using a Padlet tool. Padlet provides a cloud-based software-as-a-service, hosting a real-time collaborative web platform in which users can upload, organize, and share content to virtual bulletin boards called "Padlets”. The idea behind the workshops was to *identify ethical challenges and opportunities regarding SHAPES solutions and to define mitigation and other activities based on those challenges & opportunities (i.e., risk care).* Workshops have been a productive tool not just for identifying but also for analysing and evaluating findings and creating mitigation actions.

The role of Laurea’s participation was up to the pilot to decide. There were three different possibilities: *1) Full workshop participation 2) Retrospective participation 3) Situational participation – the pilot arranges the workshop by themselves according to instructions.*

3.1 Risk categories from SHAPES Ethical framework D8.14 Chapter 3

The Charter of Fundamental Rights of the European Union, the Convention on the Rights of Persons with Disabilities, biomedical ethics, the ethics of care, and the capabilities approach formed the basis for the SHAPES Ethical Framework in D8.4, D8.14 and also here in D8.10 as shown in Figure 4 below.



Four different focus areas:

Eu fundamental rights

Rights of the persons with disabilities

Bioethics and ethics of care

Human capabilities

3

Figure 4 Four ethical focus areas (adopted from the workshop guide)

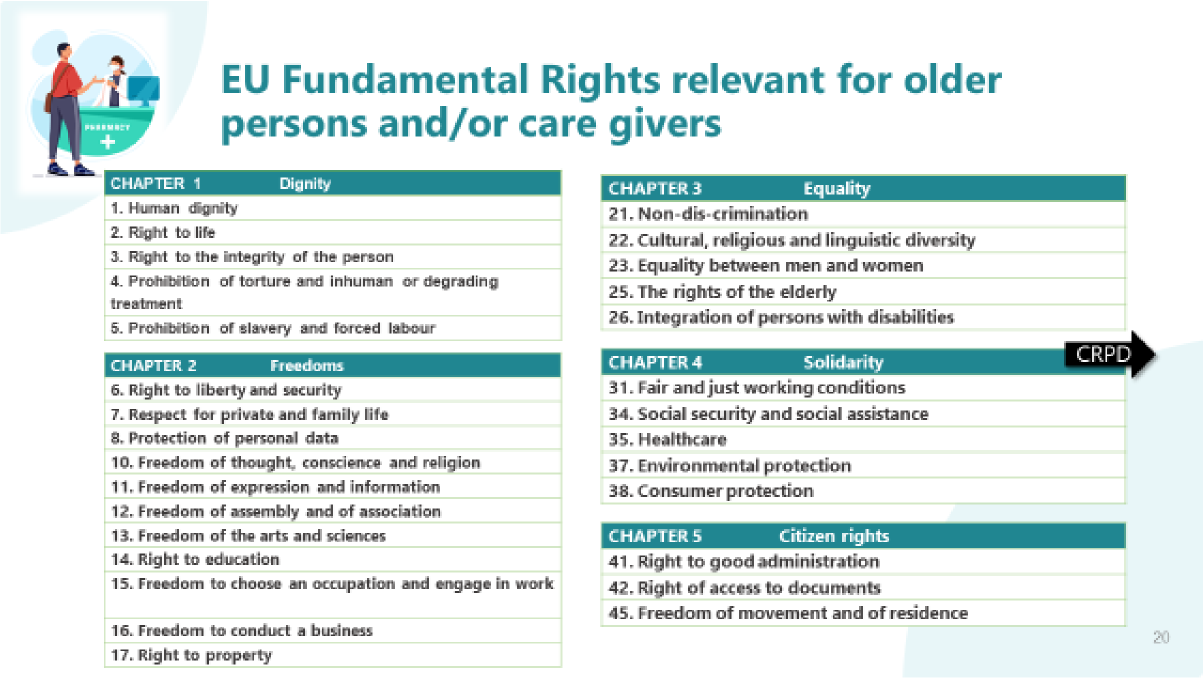
3.1.1 EU fundamental rights

The European Union (EU) is committed to upholding and promoting fundamental rights as outlined in the Charter of Fundamental Rights of the European Union. The charter, which has been legally binding since 2009, sets out a comprehensive list of civil, political, economic, and social rights that all individuals within the EU enjoy, as seen in Figure 5.

These fundamental rights are legally binding on EU institutions and member states when implementing EU law. The European Court of Justice plays a crucial role in interpreting and enforcing these rights. Member states are also required to respect and promote these rights when acting within the scope of EU law.

It is important to note that some EU member states may have additional protections for fundamental rights under their national constitutions or legal frameworks, which can complement the EU Charter of Fundamental Rights.

In D8.14 several ethical risks and opportunities related to EU Fundamental Rights were already identified and D8.9 and D8.10 continued that work.



EU Fundamental Rights relevant for older persons and/or care givers

CHAPTER 1	Dignity
1. Human dignity	
2. Right to life	
3. Right to the integrity of the person	
4. Prohibition of torture and inhuman or degrading treatment	
5. Prohibition of slavery and forced labour	

CHAPTER 2	Freedoms
6. Right to liberty and security	
7. Respect for private and family life	
8. Protection of personal data	
10. Freedom of thought, conscience and religion	
11. Freedom of expression and information	
12. Freedom of assembly and of association	
13. Freedom of the arts and sciences	
14. Right to education	
15. Freedom to choose an occupation and engage in work	
16. Freedom to conduct a business	
17. Right to property	

CHAPTER 3	Equality
21. Non-dis-crimination	
22. Cultural, religious and linguistic diversity	
23. Equality between men and women	
25. The rights of the elderly	
26. Integration of persons with disabilities	

CRPD

CHAPTER 4	Solidarity
31. Fair and just working conditions	
34. Social security and social assistance	
35. Healthcare	
37. Environmental protection	
38. Consumer protection	

CHAPTER 5	Citizen rights
41. Right to good administration	
42. Right of access to documents	
45. Freedom of movement and of residence	

20

Figure 5 EU fundamental rights (adopted from the workshop guide)

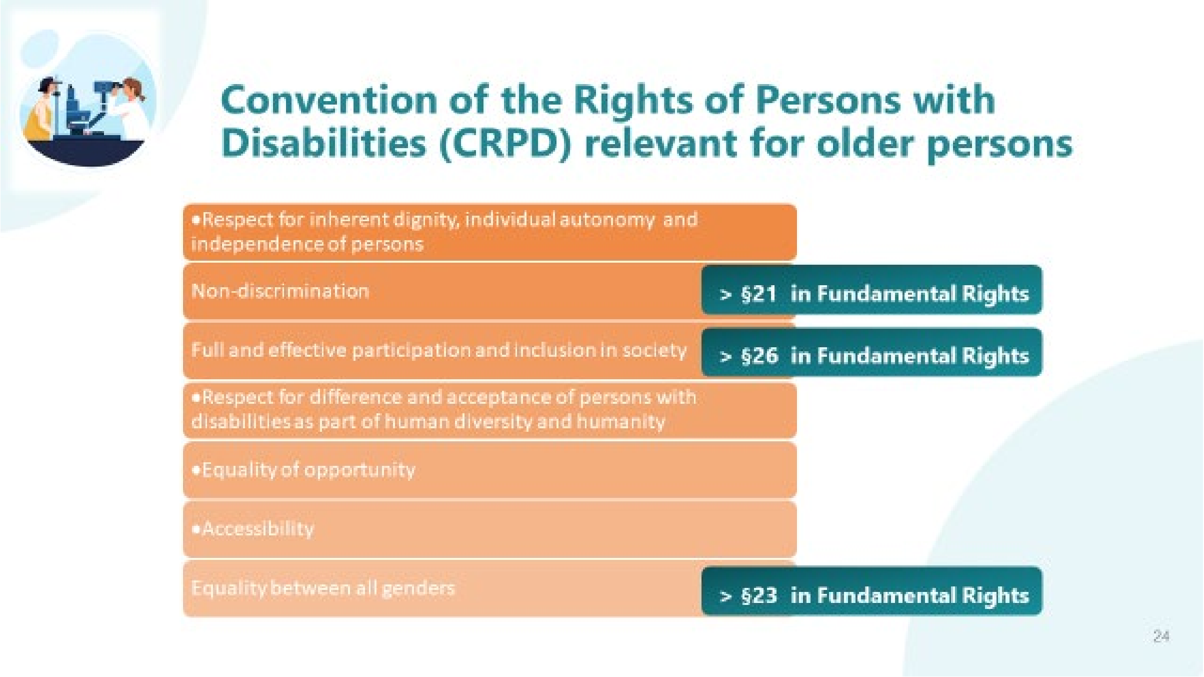
3.1.2 Rights of persons with disabilities

The Convention on the Rights of Persons with Disabilities (CRPD) is an international human rights treaty adopted by the United Nations (UN) General Assembly in 2006. It is specifically focused on promoting and protecting the rights and dignity of persons with disabilities. The CRPD is the first legally binding instrument that comprehensively

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

addresses the rights of persons with disabilities and sets out a framework for their inclusion and full participation in society.

Article 9 of the CRPD addresses accessibility 'in all its complexity' (CRPD, article 9). Accessibility must be understood more broadly than equality and non-discrimination between people. The general comment in the CRPD on Article 9 states unequivocally that accessibility must also be understood as investing in society and as part of the sustainable development agenda (CRPD/C/GC/2, paragraph 4). The products and services offered to anyone must be accessible, regardless of whether they are provided by a public authority or a private company (CRPD/C/GC/2, paragraph 13). In the SHAPES project, accessibility for potential services should be approached by assessing at least the potential gaps and risks in physical, financial, informational, and attitudinal accessibility. See the relevant sections of the CRPD as used in the workshops in Figure 6 below.



Convention of the Rights of Persons with Disabilities (CRPD) relevant for older persons

- •Respect for inherent dignity, individual autonomy and independence of persons
- Non-discrimination > §21 in Fundamental Rights
- Full and effective participation and inclusion in society > §26 in Fundamental Rights
- •Respect for difference and acceptance of persons with disabilities as part of human diversity and humanity
- •Equality of opportunity
- •Accessibility
- Equality between all genders > §23 in Fundamental Rights

24

Figure 6 Convention of the rights of person with disabilities (adopted from the workshop guide)

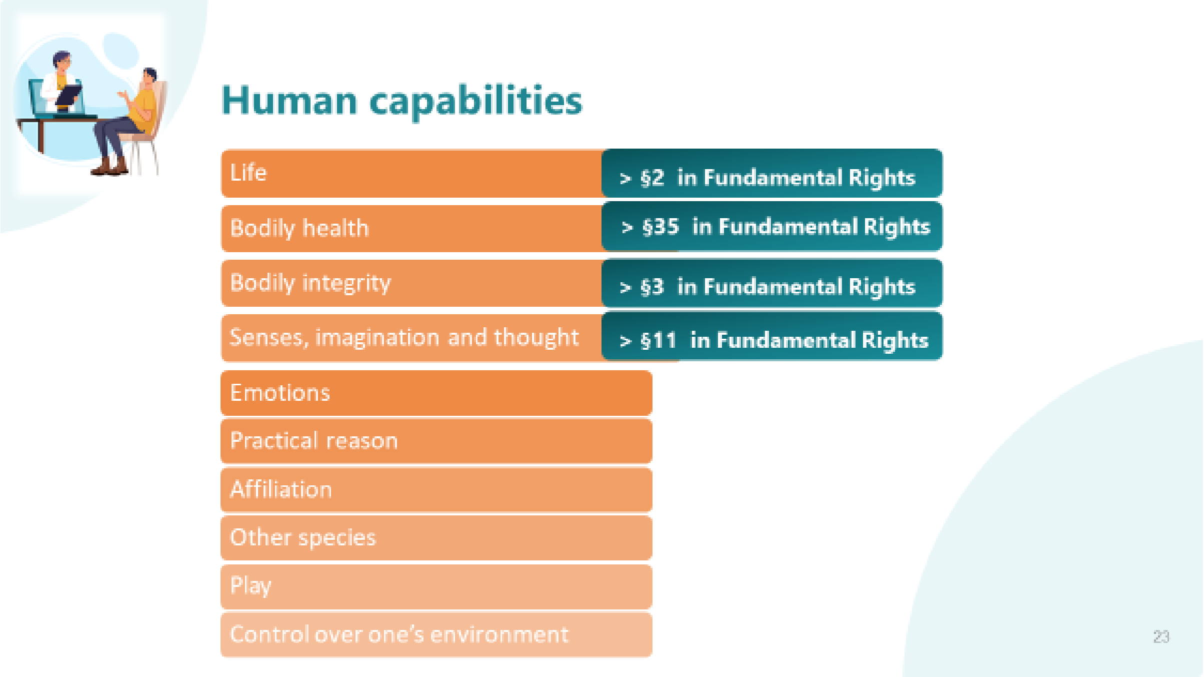
3.1.3 Capabilities approach

The capabilities approach is a theoretical framework that entails two core normative claims: 1) the freedom to achieve wellbeing is of primary moral importance, and 2) the freedom to achieve wellbeing is to be understood in terms of people's capabilities, their real opportunities to do and be what they have reason to value.

According to Nussbaum's approach, persons are both capable and needy and different in their values. However, certain capabilities and restrictions are common for people and these common features are what makes them human beings. Based on these features Nussbaum has defined a list of central human capabilities.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

These capabilities are presented as the source of political principles for a liberal pluralistic society. Nussbaum has also implied that these capabilities cover the terrain covered by both first and second generation human rights. (Nussbaum 1992; 2000; 2007 and 2011). See the list of human capabilities used in the workshops in Figure 7 below.



Human capabilities

Life > §2 in Fundamental Rights

Bodily health > §35 in Fundamental Rights

Bodily integrity > §3 in Fundamental Rights

Senses, imagination and thought > §11 in Fundamental Rights

Emotions

Practical reason

Affiliation

Other species

Play

Control over one's environment

23

Figure 7 Human capabilities (adopted from the workshop guide)

3.1.4 Bioethics and ethics of care

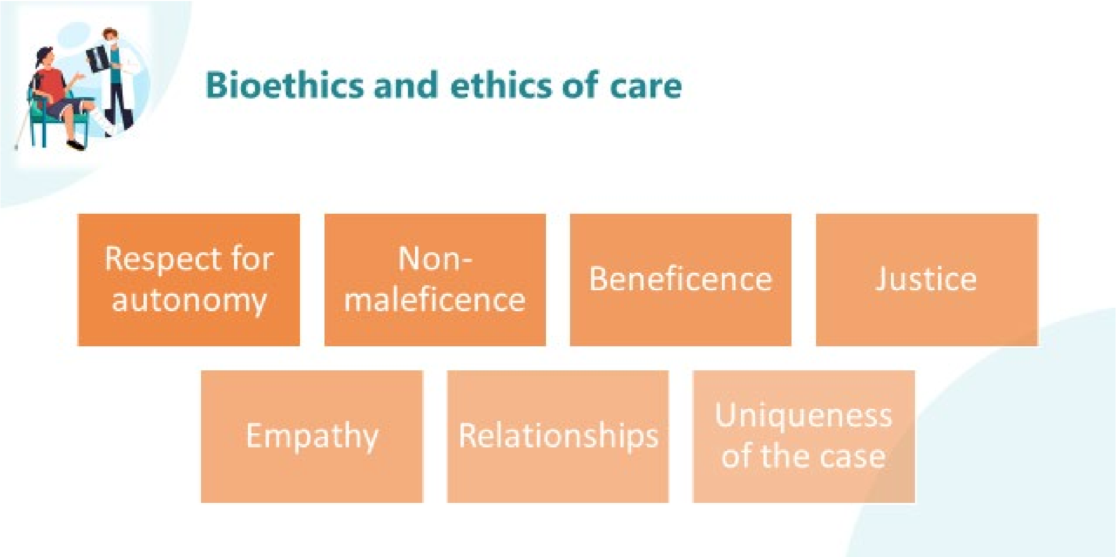
Bioethics and the ethics of care are two distinct but related approaches to moral decision-making in the context of healthcare and the life sciences. While bioethics focuses on the ethical considerations arising from advances in biology, medicine, and technology, the ethics of care places emphasis on relationships, empathy, and the particular needs and vulnerabilities of individuals.

Bioethics is a multidisciplinary field that examines the ethical implications of biomedical research, healthcare practices, and technological innovations. It involves the application of moral principles and values to address dilemmas such as patient autonomy, informed consent, resource allocation, genetic testing, end-of-life care, and medical experimentation. Bioethics draws upon various ethical theories, including utilitarianism, deontology, and virtue ethics, to analyse and provide guidance on complex moral issues in healthcare and biotechnology.

The ethics of care, on the other hand, emphasises the importance of relationships and caring practices in ethical decision-making. It emerged as a response to traditional ethical theories that were predominantly based on principles and rights. The ethics of care emphasises empathy, compassion, and the specific needs and vulnerabilities of individuals within the context of their relationships and social networks. It highlights the moral significance of personal connections, interdependence, and the responsibility to care for others, particularly those who are marginalised.

While bioethics tends to focus on broader ethical frameworks and principles, the ethics of care prioritises the concrete and contextual aspects of individual situations. The ethics of care places value on relational ethics, recognizing the interconnectedness of individuals and the significance of empathy and compassion in healthcare decision-making. It highlights the importance of listening to patients, understanding their experiences, and addressing their unique needs.

In practice, both bioethics and the ethics of care contribute valuable perspectives to moral decision-making in healthcare. Bioethics provides a systematic framework for analysing ethical issues and making principled judgments, whereas the ethics of care emphasises the importance of relationships, empathy, and context in moral deliberation. By integrating these approaches, healthcare professionals and policymakers can strive to provide ethically sound and compassionate care to individuals and communities. See a summary of the relevant sections of bioethics and ethics of care as used in the workshops in Figure 8 below.



Bioethics and ethics of care

Respect for autonomy

Non-maleficence

Beneficence

Justice

Empathy

Relationships

Uniqueness of the case

Figure 8 Bioethics and the ethics of care (adopted from the workshop guide)

3.2 *Identified risks from the viewpoint of the main activities of SHAPES*

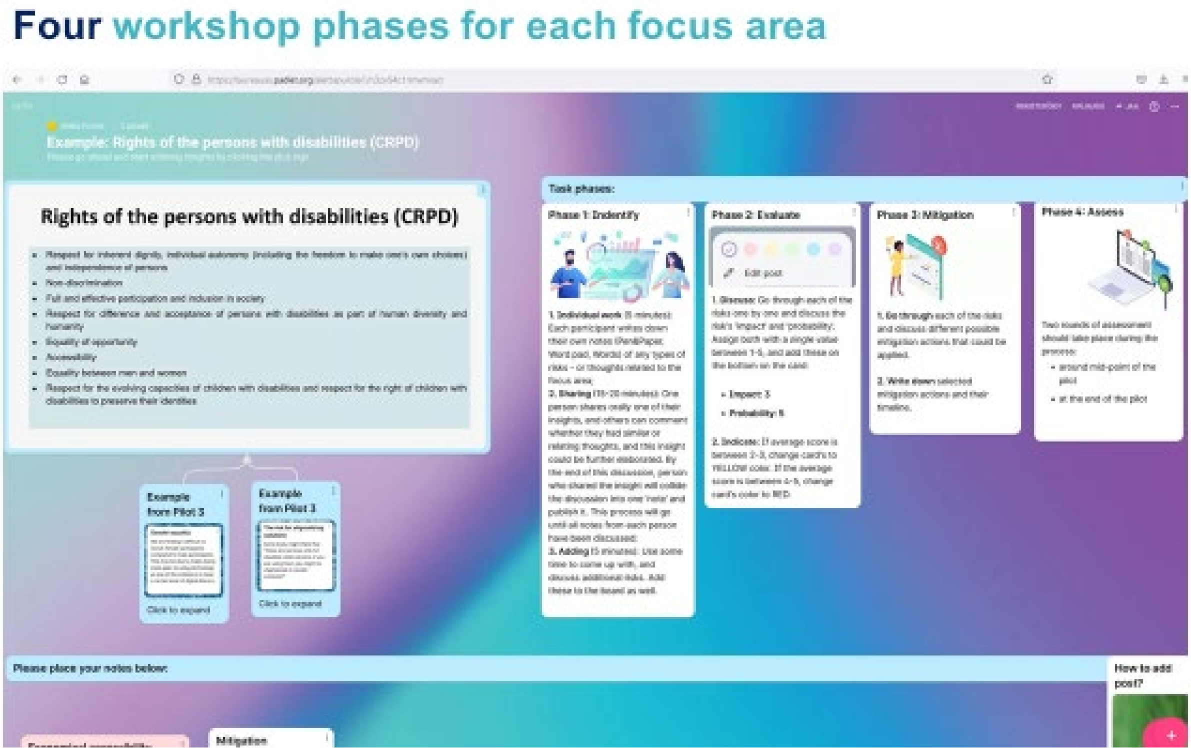
From the implementation of the workshops:

1. The risk analysis is based on material collected from the workshops of seven different pilots and their expert networks. The workshops were organised by Laurea University of Applied Sciences, and they were carried out between June 2022 and January 2023.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

2. The workshops were implemented online in Padlet. The experts considered various ethical risks related to the project's technology pilots for older persons, especially from the point of view of EU fundamental rights, bioethics, human capacities, and GDPR.

Workshop directions and a short summary of each framework were provided in a Padlet tool as shown in Figure 9 below.



Four workshop phases for each focus area

Example: Rights of the persons with disabilities (CRPD)

Rights of the persons with disabilities (CRPD)

- Respect for inherent dignity, individual autonomy (including the freedom to make one's own choices) and independence of persons
- Non-discrimination
- Full and effective participation and inclusion in society
- Respect for difference and acceptance of persons with disabilities as part of human diversity and humanity
- Equality of opportunity
- Accessibility
- Equality between men and women
- Respect for the evolving capacities of children with disabilities and respect for the right of children with disabilities to preserve their identities

Example from Pilot 3

Click to expand

Example from Pilot 3

Click to expand

Task phases:

Phase 1: Indentify

1. **Individual work** (5 minutes): Each participant writes down their own notes (Pen&Paper, Word pad, Words) of any types of risks – or thoughts related to the focus area;
2. **Sharing** (15-20 minutes): One person shares orally one of their insights, and others can comment whether they had similar or relating thoughts, and this insight could be further elaborated. By the end of this discussion, person who shared the insight will collate the discussion into one 'note' and publish it. This process will go until all notes from each person have been discussed;
3. **Adding** (5 minutes): Use some time to come up with, and discuss additional risks. Add these to the board as well.

Phase 2: Evaluate

1. **Discuss:** Go through each of the risks one by one and discuss the risk's 'impact' and 'probability'. Assign both with a single value between 1-5, and add these on the bottom on the card:

- **Impact:** 3
- **Probability:** 5

2. **Indicate:** If average score is between 2-3, change card's to YELLOW color. If the average score is between 4-5, change card's color to RED.

Phase 3: Mitigation

1. **Go through** each of the risks and discuss different possible mitigation actions that could be applied.
2. **Write down** selected mitigation actions and their timeline.

Phase 4: Assess

Two rounds of assessment should take place during the process:

- around mid-point of the pilot
- at the end of the pilot

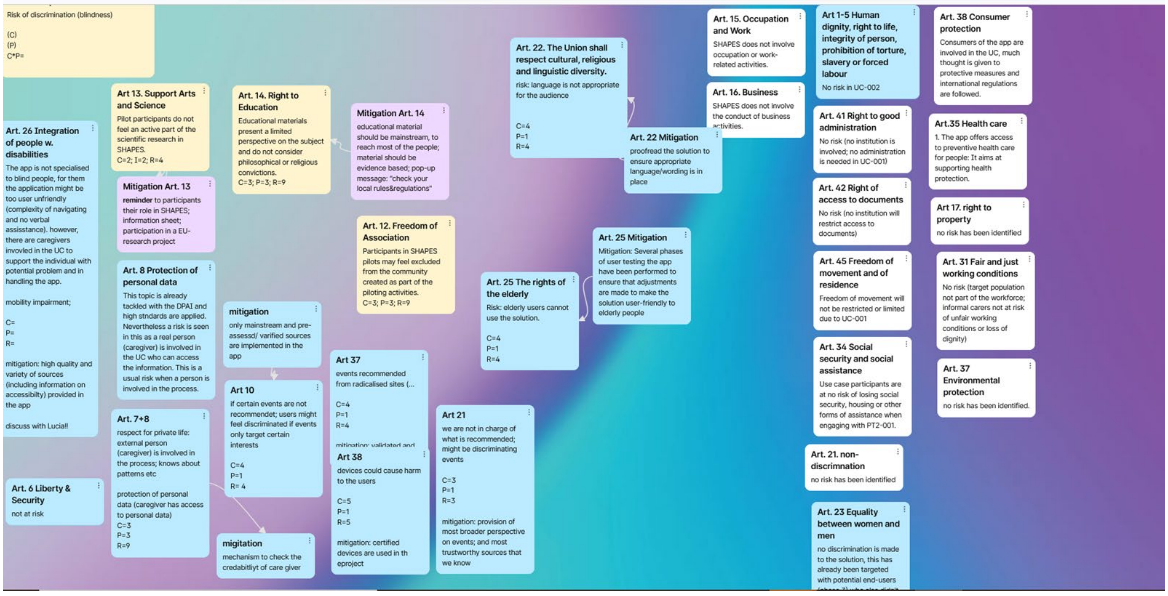
Please place your notes below:

How to add post?

Figure 9 Example of a Padlet view

The Padlet tool enabled co-creative working online in the workshops as shown in Figure 10 below.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159



Risk of discrimination (blindness)

(C)
(P)
C*P=

Art. 26 Integration of people w. disabilities
The app is not specialised to blind people, for them the application might be too user unfriendly (complexity of navigating and no verbal assisstance). however, there are caregivers invovled in the UC to support the individual with potential problem and in handling the app.

mobility impairment;

C=
P=
R=

mitigation: high quality and variety of sources (including information on accessibilty) provided in the app

discuss with Lucia!!

Art. 6 Liberty & Security
not at risk

Art 13. Support Arts and Science
Pilot participants do not feel an active part of the scientific research in SHAPES.
C=2; I=2; R=4

Mitigation Art. 13
reminder to participants their role in SHAPES; information sheet; participation in a EU-research project

Art. 8 Protection of personal data
This topic is already tackled with the DPAI and high stndards are applied. Nevertheless a risk is seen in this as a real person (caregiver) is involved in the UC who can access the information. This is a usual risk when a person is involved in the process.

Art. 7+8
respect for private life: external person (caregiver) is involved in the process; knows about patterns etc

protection of personal data (caregiver has access to personal data)
C=3
P=3
R=9

Art. 14. Right to Education
Educational materials present a limited perspective on the subject and do not consider philosophical or religious convictions.
C=3; P=3; R=9

mitigation
only mainstream and pre-assessd/ varified sources are implemented in the app

Art 10
if certain events are not recommendet; users might feel discriminated if events only target certain interests

C=4
P=1
R= 4

migitation
mechanism to check the credabitliyt of care giver

Mitigation Art. 14
educational material should be mainstream, to reach most of the people; material should be evidence based; pop-up message: "check your local rules&regulations"

Art. 12. Freedom of Association
Participants in SHAPES pilots may feel excluded from the community created as part of the piloting activities.
C=3; P=3; R=9

Art 37
events recommended from radicalised sites (...

C=4
P=1
R=4

mitigation: validated and

Art 38
devices could cause harm to the users

C=5
P=1
R=5

mitigation: certified devices are used in th eproject

Art 21
we are not in charge of what is recommended; might be discriminating events

C=3
P=1
R=3

mitigation: provision of most broader perspective on events; and most trustworthy sources that we know

Art. 22. The Union shall respect cultural, religious and linguistic diversity.
risk: language is not appropriate for the audience

C=4
P=1
R=4

Art. 22 Mitigation
proofread the solution to ensure appropriate language/wording is in place

Art. 25 The rights of the elderly
Risk: elderly users cannot use the solution.

C=4
P=1
R=4

Art. 25 Mitigation
Mitigation: Several phases of user testing the app have been performed to ensure that adjustments are made to make the solution user-friendly to elderly people

Art. 15. Occupation and Work
SHAPES does not involve occupation or work-related activities.

Art. 16. Business
SHAPES does not involve the conduct of business activities.

Art 1-5 Human dignity, right to life, integrity of person, prohibition of torture, slavery or forced labour
No risk in UC-002

Art. 41 Right to good administration
No risk (no institution is involved; no administration is needed in UC-001)

Art. 42 Right of access to documents
No risk (no institution will restrict access to documents)

Art. 45 Freedom of movement and of residence
Freedom of movement will not be restricted or limited due to UC-001

Art. 34 Social security and social assistance
Use case participants are at no risk of losing social security, housing or other forms of assistance when engaging with PT2-001.

Art. 21. non-discrimnation
no risk has been identified

Art. 23 Equality between women and men
no discrimination is made to the solution, this has already been targeted with potential end-users

Art. 38 Consumer protection
Consumers of the app are involved in the UC, much thought is given to protective measures and international regulations are followed.

Art.35 Health care
1. The app offers access to preventive health care for people: It aims at supporting health protection.

Art 17. right to property
no risk has been identified

Art. 31 Fair and just working conditions
No risk (target population not part of the workforce; informal carers not at risk of unfair working conditions or loss of dignity)

Art. 37 Environmental protection
no risk has been identified.

Figure 10 An example of workshop findings

The data from the workshops was first divided into the following topics:

- Growing inequality
- Dehumanisation of care
- Access to ethically sustainable services
- Data protection and information security issues
- Independency & Autonomy

At the end of the chapter, Table 16 shows more examples of findings and their mitigation.

3.3 Thematic division of the risks and opportunities

The various themes were condensed into four themes. According to the results, the risks associated with technology are, among others, data protection and information security issues, growing inequality, dehumanisation of care, and access to ethically sustainable services. The need for sufficient support services and user driven development should be taken into account at all times. However, the respondents also emphasised that SHAPES aims to support the independence and autonomy of sensitive user groups. See Figure 11 below for the general ethical risks that emerged from the workshops.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

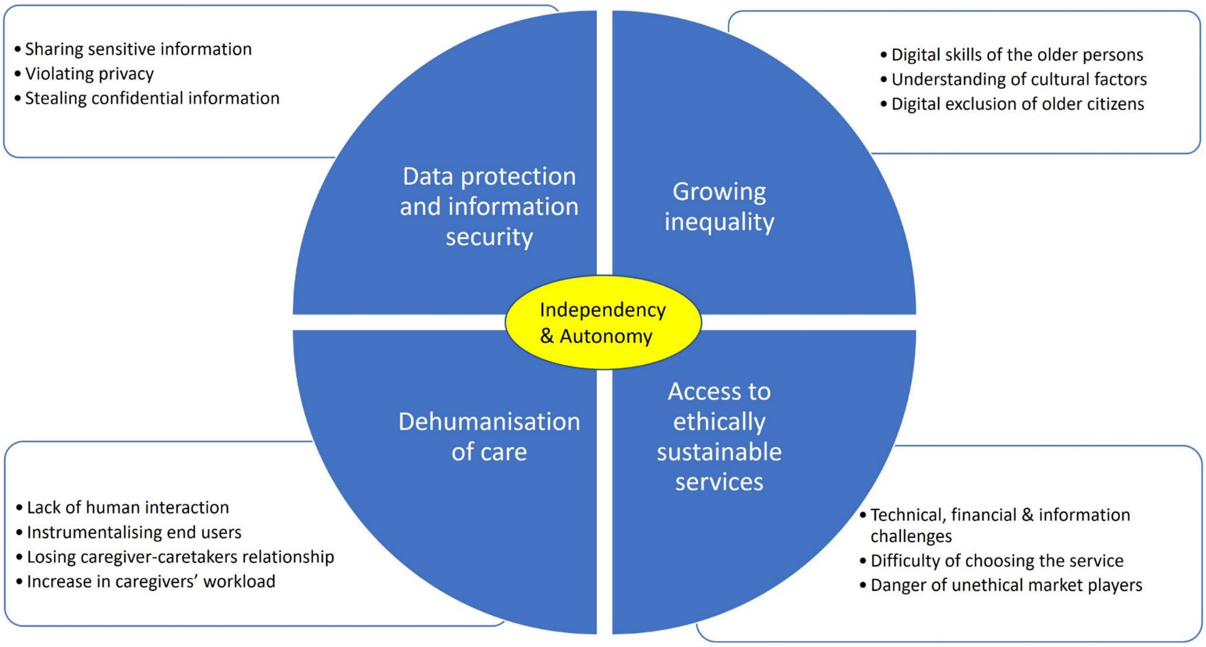

• Sharing sensitive information
• Violating privacy
• Stealing confidential information
Data protection and information security
Growing inequality
• Digital skills of the older persons
• Understanding of cultural factors
• Digital exclusion of older citizens
Independency & Autonomy
Dehumanisation of care
Access to ethically sustainable services
• Lack of human interaction
• Instrumentalising end users
• Losing caregiver-caretakers relationship
• Increase in caregivers' workload
• Technical, financial & information challenges
• Difficulty of choosing the service
• Danger of unethical market players

Figure 11 Themes of ethical risk

3.3.1 Growing inequality

According to the workshops, common ethical risks were **digital skills of older persons**, **understanding cultural factors,** and **digital exclusion of older citizens**. The experts talked about the risks related to the digital skills of older persons. The digital solutions employed require a certain level of digital literacy. The respondents were concerned about the effects of the end-users' lack of digital skills on senior citizens' full participation in the digitising society and access to services. When planning digital services, users' different digital skills must be taken into account. Otherwise, the digital services will remain unused, and inequality will increase. Cultural factors were often mentioned. Ignoring cultural factors, such as language and music, negatively affects technology adoption and user experience. Digital exclusion of older citizens was described e.g., as exclusion from services and the digitising society and non-realization of civil rights. An example was used of the non-realization of full citizenship rights during the COVID passport process. The experts described the risk like this:

> *"Suppression of one's right to stay in non-digital world (already seen with COVID passports). Both from the perspective of low lit*eracy, or from the perspective of self-privacy."

The themes of growing inequality are listed in Table 5 below.

Table 5 Themes of growing inequality

Themes of growing inequality
Digital skills of the older persons
Understanding of cultural factors
Digital exclusion of older citizens

3.3.2 Unethical services vs access to ethically sustainable services

Ethical risks related to the accessibility of services appeared as **technical**, **financial,** and **informational** challenges, **the difficulty of choosing a suitable service,** and **the danger of unethical market players** (see Table 6). Digital solutions often require the use of personal tablets/smartphones and Wi-Fi, which require funding for new technology and technical know-how. Service systems were always seen to have a political dimension as well. It was also mentioned in the workshops that the government often tends to force users (citizens) to use one type of digital solution without the possibility of using alternatives. In this case, some citizens may have financial challenges using the services. In addition, the experts stated that it is difficult for older persons to choose a suitable and safe service that meets their care needs. The danger of unethical market players and so-called "eHealth" digital solutions, which do not have solid scientific evidence, were also seen as one risk.

However, the SHAPES project was also seen to have a positive potential to improve the availability of services, as it promotes more demand-oriented health care. The experts also saw that it is possible that the physical and cognitive health of the older people who participated in the project will improve by using these pilot digital solutions - even if digital solutions do not replace healthcare know-how and care.

Table 6 Challenges of ethically sustainable services

Themes
Technical, financial and informational challenges
The difficulty of choosing a suitable service
The danger of unethical market players

3.3.3 Dehumanisation of care

From the caregivers' point of view, the ethical risks were a lack of human interaction, instrumentalizing end users, losing caregiver-caretaker relationship, and an increase in the caregiver's workload. According to the workshops, digital solutions and their functionalities may increase caregivers' everyday workload. In addition, the reduction of traditional face-to-face care chains may weaken the well-being of caregivers and those being cared for. Lack of human interaction was described as the exhaustion of human-centred planning, where interaction with people is not considered enough as part of the solution. The themes of dehumanisation of care are listed in Table 7 below.

Table 7 Themes of dehumanisation of care

Themes of dehumanisation of care
Lack of human interaction
Instrumentalizing end users
Losing caregiver-caretaker relationship
Increase in the caregiver's workload

3.3.4 Data protection and information security

Privacy, data protection, security, and data management issues must be taken care of with special care in all services related to the health and well-being of sensitive end users. **GDPR risks** were identified as **sharing sensitive information**, **violating privacy,** and **stealing confidential information.** This theme is discussed in more detail in the next chapter of the report. The themes of data protection and information security are listed in Table 8 below:

Table 8 Themes of data protection and security

Themes of data protection and security
Sharing sensitive information
Violating privacy
Stealing confidential information

3.3.5 Loss of independence and autonomy

There was general emphasis also that SHAPES should aim to support the independence and autonomy of sensitive user groups. It is important to ensure that older individuals have the right to make informed decisions about their choices without undue influence or coercion.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

Respect for autonomy can be hurt if there is, for example, a need to perform specific tasks in a specific timeline (e.g., dance 5 songs during the course of a week). This could be seen as an obligation by the user and disruptive of their daily routine.

> *“Initially, we defined the level of difficulty that the participant would use. Then we changed our approach to respect the participant's autonomy to play the level they want to (even if they have the worst performance results).”*

This is also linked to the choice of the services and end-users’ possibility to choose or not to choose a service. **Having control over One’s environment** was seen as important in expert groups. See the thematic table of analysis below (Table 9).

Table 9 Themes of independency and autonomy

Themes of independence and autonomy
Respect for autonomy
Freedom of choice regarding the services to be used
Control over One’s Environment

3.4 Themes of risks mitigation

The workshops stated that a certain level of risk must be taken into account when planning digital services. One has to remember that not only risks, but opportunities as well are mapped during workshops. It is impossible to develop a completely risk-free ecosystem. However, there are many risk-mitigating measures that can be taken. Figure 12 summarises the key risk mitigation themes of the pilots.

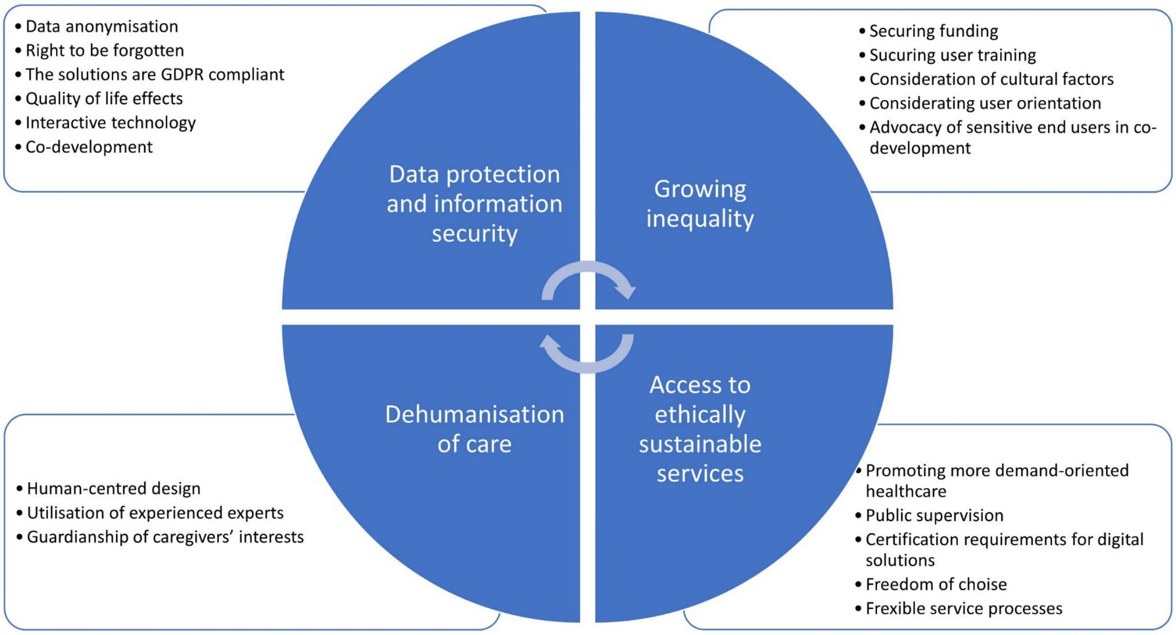

• Data anonymisation
• Right to be forgotten
• The solutions are GDPR compliant
• Quality of life effects
• Interactive technology
• Co-development
Data protection and information security
Growing inequality
• Securing funding
• Sucuring user training
• Consideration of cultural factors
• Considerating user orientation
• Advocacy of sensitive end users in co-development
Dehumanisation of care
• Human-centred design
• Utilisation of experienced experts
• Guardianship of caregivers' interests
Access to ethically sustainable services
• Promoting more demand-oriented healthcare
• Public supervision
• Certification requirements for digital solutions
• Freedom of choise
• Frexible service processes

Figure 12 Themes of risk mitigation

3.4.1 Growing inequality

In order to mitigate the risk of **growing inequality**, (see Table 10), efforts must be made to ensure fair funding, to ensure user education, and to take cultural factors into account in planning. According to experts, taking cultural factors into account also affects the adoption of technology and enables a positive user experience:

> *"Pay attention to cultural or language differences in participating countries, such as gender-appropriate language, capitalization, and the use of lowercase letters."*

To experts, it is important to ensure user education to **prevent digital exclusion**. It is essential to improve the digital health literacy of individuals so that they can access digital health services. The different needs and functional limitations of the users must also be taken into account. It is important to consider user orientation and the protection of interests of sensitive end users in co-development. Although joint development was seen as important, there are also risks that must be critically evaluated.

> *“The interests of co-creating better services must be critically evaluated, in order for the end users' participation in development not to be exploited uncritically. Positive change must also be of advantage to them.”*

Table 10 Mitigation measures, growing inequality

Mitigation measures
Securing funding
Securing user training
Consideration of cultural factors
Considering user orientation
Advocacy of using end users in co-development

3.4.2 Dehumanisation of care

In order to **avoid the dehumanisation of care**, more human-centred planning (see Table 11) and the use of experienced experts are needed as guardians of the caregivers' interests. The experts mentioned human-centred design as follows:

> *"Human-centred design considers interaction with human-beings as an important part of the solution."*

In order to ensure **human-centric care**, the knowhow of experienced experts should be utilised, and the interest organisations of sensitive customer groups should be involved in the joint development. It also must be ensured that the functionalities do not increase the workload for the caregivers' everyday life. One possible way to avoid this is to use robots as a way for older persons to stay in contact with people. However, it must be ensured that there are processes in place that allow participants to link with health care provision face-to-face if they wish. The experts described mitigating the risk like this.

> *"Ensure that processes are in place to enable participants to link into/access face to face healthcare provision if that is preferred."*

Table 11 Mitigation measures, dehumanisation of care

Mitigation measures
Human-centred design
Utilisation of experienced experts
Guardianship of caregivers interest
Human-centred design
Utilisation of experienced experts

3.4.3 Privacy and Data protection

In order to mitigate the risk of **data security and protection**, the anonymization of data must be ensured, as well as the right to be forgotten and it must be ensured that solutions are GDPR compliant. In addition, solutions must support evaluating effects on quality of life and increase interactive technology and opportunities for co-development.

> *"Discuss and understand the tradeoffs between benefits for health and quality of life vs drawbacks such as privacy reduction sufficiently well."*

The experts pointed out that it is important for older people to understand and accept where and how information is collected and with whom it is shared. Voluntary and informed consent must be obtained from them for the collection and possible sharing of information (including sharing with loved ones).

According to experts, the right to shut down the systems, if desired, is also key. In addition, end users must have the right to receive information about the collected results. Users should also be able to activate the data collection of applications manually. Also, in the context of the project, it was considered important to ensure that the SHAPES solutions and pilots are GDPR compliant. Information collected from pilot workshops suggests the following mitigation measures, see Table 12.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

Table 12 Mitigation measures, privacy and data protection

Mitigation measures
1. It is important that older people understand and accept where and how information is collected and with whom it is shared.
2. Voluntary and informed consent to data collection and possible sharing must be obtained from them (also sharing with loved ones).
3. Co-design.
4. The right to be reported about results
5. Right to disconnect systems when desired.
6. Users should be able activate the data collection of applications manually.
7. It should be ensured that SHAPES solutions and pilots comply with GDPR.
8. The use of less invasive sensor technology.
9. Careful evaluation of the benefits and harms to health and quality of life, such as reduced privacy: Which causes less harm and more benefits?
10. Ethically sustainable user-oriented design.

3.4.4 The choice and accessibility of the services

In order to mitigate (Table 13) the risk of **access to ethically sustainable services**, more demand-oriented health care should be promoted, public supervision of private services ensured, certification requirements for digital solutions prepared, end users' freedom of choice added, and more flexible service developed. According to experts, digital applications and services need more flexible guidelines that respect end users' right to self-determination. The importance of freedom of choice in the use of services was also emphasised.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

Table 13 Mitigation actions

Mitigation actions
1. Flexible guidelines that respect end users' right to self-determination
2. Freedom of choice in the use of services
3. End users' option for face-to-face service (not either/or but both)
4. Certification requirements for digital solutions
5. Public supervision
6. Ethically sustainable user-oriented design

3.4.5 Promoting Independence and autonomy

Enabling independence and autonomy in SHAPES was considered to be an important and shared goal. SHAPES should prioritize autonomy and well-designed informed consent procedures for older adults. It is essential to provide clear information about the purpose, benefits, and risks associated with using SHAPES services, and ensure that older individuals have the right to make informed decisions about their healthcare without undue influence or coercion.

The technological solution used must be adapted to the participant's physical conditions. For example, people who have sensory problems (low visual acuity) may be frustrated with badly designed user interfaces. This can be a stigmatising factor and hurt autonomy. See mitigation themes below in Table 14.

Table 14 Themes of mitigation

Themes of mitigation
Provide clear and accessible information about the benefits, risks, and limitations of digital services, enabling them to make informed decisions about their healthcare.
Ensure that older individuals have the freedom to choose whether to use digital services or opt for alternative options, without coercion or pressure.
Co-create with end-users

3.4.6 Some specific risks that were discussed in detail

Some other more specific risks and opportunities were raised and discussed so much in detail in most of the workshops that they are worth bringing up.

3.4.6.1 Governance and business model risks

Many risks connected to access to sustainable services can be related to governance and business models. The experts talked about the risks related to the digital skills of older individuals, the difficulty of choosing a suitable and safe service that meets the need for care, and the danger of unethical market players in digital solutions. However, the experts saw that it is possible that the physical and cognitive health of the older people who participated in the project will improve by using these pilot digital solutions—even if the digital solutions do not replace healthcare know-how and care. Examples of solutions to this can be seen in Table 15.

Table 15 Solutions to the risks and opportunities suggested by experts

The expert suggested solutions to the risks
Joint planning
Securing end user rights and freedom of choice
Certification requirements for digital solutions and public supervision
Securing funding
Securing user training to prevent digital exclusion
Ethically sustainable user-oriented design

3.4.6.2 Co-creation risks

The observed co-creation risks were committing participants to development, ensuring continuous evaluation and instrumentalizing end users. The experts saw the importance of continuous and agile monitoring, as well as evaluation and development together with end users. However, the interests of co-creating better services must be critically evaluated in order for end users' participation in development not to be exploited uncritically. Positive change must also be of advantage to them. This risk was described, for example, as follows:

> *“Do we see participants only as instruments to develop better services, or are they really empowered to make a change with us?“*

3.4.6.3 Risks from caregivers’ viewpoint

From the caregivers' point of view, the ethical risks were the increase in caregivers' workload, the dehumanisation of care giving and the decrease in human interaction. To mitigate these risks, it must be ensured that functionalities do not increase the workload of caregivers' everyday life. In addition, it should be possible to choose and

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 857159

reach traditional face-to-face care chains, if necessary. Human-centred design was also emphasised, where interaction with people is an important part of the solution.

In Table 16, there are multiple examples of risks, opportunities and mitigation that were raised in workshops.

Table 16 The data from the pilots' risk workshops (examples)

Category	Risk	Mitigation
General	Cultural factors	Consideration of cultural factors
Tailored for cultural issues	Technological information is ununderstood wrong. *"The language used by technology must be culturally adapted (education, gender, religion, other cultural specification)."* *"Pay attention to differences in culture or language within participating countries, e.g., gender-appropriate language, capitalization & use of small letters"*	Cultural translations Ensuring that the digital solution allows a choice of songs that relate to the user's culture.
Co-creation with end users and other stakeholders	Co-creation	Co-development
Full and Effective Participation **Continuous evaluation, monitoring and development**	Risk of users not being able to understand the DS and critically think of them, thus not being adequately engaged with the pilots. *"Do we see participants only as instruments to develop better services, or are they really empowered to make a change with us? "*	User engagement from the early start of the DS; hands-on training and user feedback through time to improve functionality, friendliness and usefulness. **Involve users in the design and development of the solution from the beginning. Agile methodology.**
Privacy, data protection, security and data management		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

Data protection and information security risks ***"Risk that participants don't feel comfortable sharing their personal information (thoughts and beliefs) in front of their relatives or carers."***	Rick of sharing confidential data during pilots (unauthorised access). Personal data can be stolen or accessed by people outside the project. The risk that the older persons do not understand what information is collected and with whom it is shared. Use of technologies in the home environment to identify daily activities and habits can be perceived as a threat to the respect for the private and family life, as well as the protection of personal data.	Data collection by apps should be activated manually by users. Ensuring that SHAPES solutions and pilots respect the GDPR. To explain to the participants that they will not be made aware of the health risk predictors and that these predictors will be reviewed/ processed by the research team to ensure that the technology works well. 1. Co-design users may choose which sensors they want to be installed. 2. Use of less invasive sensor technologies (i.e., presence sensor vs camera). 3. Discuss and understand the tradeoffs between benefits for health and quality of life vs drawbacks such as privacy reduction sufficiently well.
Caregivers	Dehumanisation of care	Dehumanisation of care
Professional caregivers' workload **Family caregivers' viewpoint** **Relationships** ***"Some of the dance mat users say that they use it to play with their grandchildren"***	Un-intended /unidentified impact on caregiver's workload (article 31, fair and just working conditions). Risk that digital technologies could be seen as a substitute for human interactions with healthcare providers. A social robot may de-humanise the caregiver-caretaker relationship. On some occasions, there may be the risk that having a robot as the only interaction	DS should assure that functionalities do not put more work on their shoulders. Ensuring that processes are in place to enable participants to link into/access face to face healthcare provision if that is preferred. One possible way to avoid this is to use the robot also as a way for the older person to stay in contact with people.

	partner may exacerbate the feeling of loneliness. Risk: Technology solutions reduce human interaction. The user feels the technology will reduce visits of relatives, medical appointments.	Mitigation: human-centred design considering interaction with human-beings as an important part of the solution.

3.5 Discussion on ethics risks with Laurea R&D people

Laurea arranged a workshop on May 8, 2023, with Laurea health care specialists concerning the ethical risks and opportunities identified by SHAPES pilots in the workshops. The idea was to discuss categorised analysis of these and see if experts could further bring mitigation ideas from their experience. Themes of growing inequality, access to services, and dehumanisation of care gave the most results.

On the Growing inequality among other issues, there was concern that some older persons do not know how to behave on the internet and social media, and how to avoid risks there. This may also decrease reliance on digital services.

On Access to sustainable services, there were worries concerning that terms and conditions are difficult to read even when not having diminished cognitive capacity and that unethical market players are an essential risk. This risk is especially related to AI and to data protection.

On the dehumanisation of care, there was a discussion on the overuse of technology. This was considered a risk in the era of diminishing care workers and diminishing money in the welfare state to provide services.

As can be seen, topics in challenges and as mitigation activities are mainly overlapping with results from SHAPES pilots' workshops.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

4 Risks related to the use of Artificial Intelligence

4.1 The risk identification and mitigation process

The Assessment List for Trustworthy Artificial Intelligence (ALTAI):

- The Assessment List for Trustworthy AI (ALTAI) was developed by the High-Level Expert Group on Artificial Intelligence set up by the European Commission to help assess whether an AI system that is being developed, deployed, procured or used, complies with the seven requirements of Trustworthy AI, as specified in our Ethics Guidelines for Trustworthy AI.
- ALTAI was presented to the SHAPES partners and pilot leaders in different meetings under WP8 during the spring and autumn of 2022.
- Pilot leaders filled in ALTAI questionnaires on behalf of their AI applications (technology providers had already answered these but most of the AI ethical challenges are related to actual use cases).
- During 11/2022 – 05/2023 the results were elaborated further with pilots 5,6 and 7. The work was done by the Laurea team and the leaders of pilots 5, 6 and 7.
- Results will be reported in D8.10 and in the article ALTAI Tool for Assessing AI-Based Technologies: Lessons Learned and Recommendations from SHAPES Pilots (Authors: Jyri Rajamäki, Fotios Gioulekas, Pedro Rocha, Xavier del Toro Garcia, Paulinus Ofem and Jaakko Tyni).

4.2 ALTAI recommendations

A cross-case analysis (Figure 13) was carried out using the responses provided by the partners of the pilots to understand the similarities and differences among the pilots (case studies). Overall, the assessment indicates that the highest score was achieved in terms of "transparency," while the lowest score was attributed to "technical robustness and safety." Additionally, each partner has been provided with a set of recommendations.

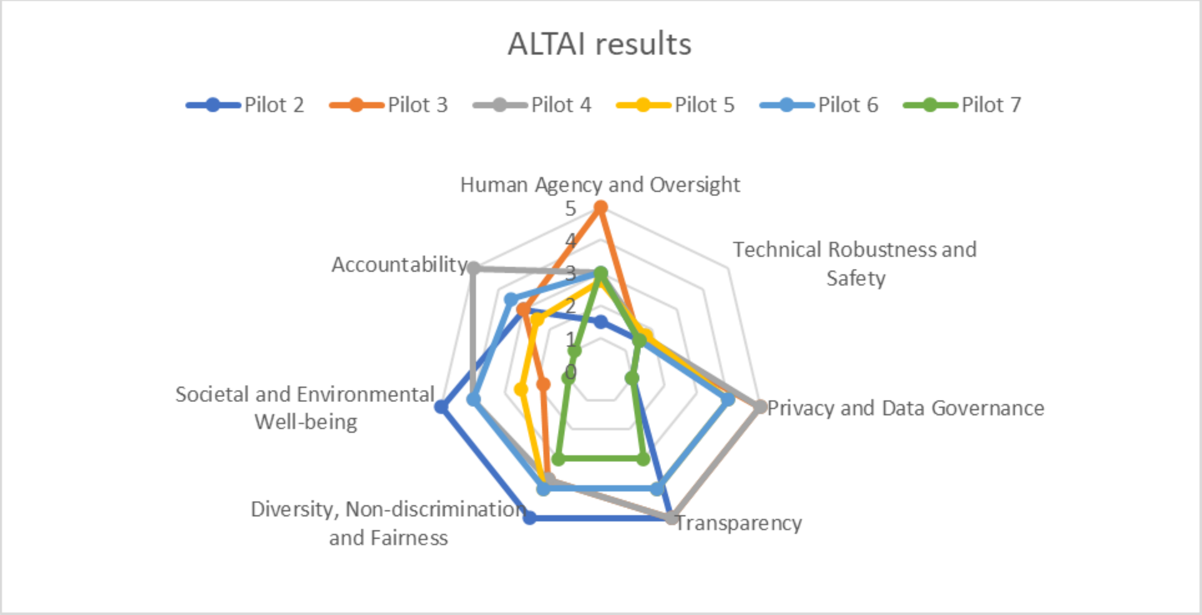


Figure 13 ALTAI self-assessment results per SHAPES pilot and cross-analysis

4.2.1 Human agency and oversight

Four recommendations were provided for multiple pilots. These recommendations were intended to discourage excessive reliance on the system, prevent inadvertent effects on human autonomy, and provide appropriate training and oversight to individuals responsible for monitoring the system's decisions. Pilot 3 was recommended to implement a “stop button” or procedure to safely terminate an operation when necessary. Pilot 5 did not get any recommendations for this requirement.

4.2.2 Technical robustness and safety

Pilots 2 and 5 were recommended to evaluate possible types of attacks that the AI system may be susceptible to. Pilot 5 received four suggestions aimed at identifying and mitigating risks related to the utilisation of AI systems. These recommendations encompass the identification of potential attacks and threats, addressing the potential consequences of system failure or malfunction, and emphasising the importance of continuous monitoring and evaluation to ensure the technical robustness and safety of the system. Pilots 3, 4, 5 and 7 got no recommendations for this requirement.

4.2.3 Privacy and Data Governance

Four recommendations were provided for multiple pilots, including considerations for privacy and data protection throughout the employed AI system's life cycle, alignment with relevant standards and protocols, implementation of rights such as consent withdrawal and objection, and the establishment of mechanisms for flagging privacy or data protection issues in the AI system. Furthermore, pilot 7 was advised to take into account the privacy and data protection implications associated with the AI system's non-personal training data or any other processed non-personal data. Pilots 4 and 5 got no recommendations for this requirement.

4.2.4 Transparency

Pilots 2, 3, 5 and 6 were recommended to regularly survey users to ensure they understand the decisions of the AI systems. Pilots 2, 6 and 7 were advised to consider informing the users that they are engaging with a machine. Pilots 2 and 6 were proposed to take steps to continuously assess the quality of input data used by their AI systems. Pilot 6 was advised to consider providing explanations of the decisions adopted or recommended by the AI system to its end users. Pilot 4 received no recommendation for this requirement.

4.2.5 Diversity, non-discrimination and fairness

This requirement got the most recommendations, a total of 90 recommendations. The recommendation to establish mechanisms that guarantee fairness within their AI systems was received by all the pilots. Recommendations that were given to two or more pilots can be further divided into the following subcategories:

1. Data and algorithm design: This includes recommendations related to the input data and algorithm design used in the AI system, such as avoiding bias and ensuring diversity and representativeness in the data, using state-of-the-art technical tools to understand the data and model, and testing and monitoring for potential biases throughout the AI system's life cycle.
2. Awareness and education: This includes recommendations related to educating AI designers and developers about the potential for bias and discrimination in their work, establishing mechanisms for flagging bias issues, and ensuring that information about the AI system is accessible to all users, including those with assistive technologies.
3. Fairness definition: This includes recommendations related to defining fairness and consulting with impacted communities to ensure that the definition is appropriate and inclusive. It also includes suggestions for establishing quantitative metrics to measure and test the definition of fairness.
4. Risk assessment: This includes recommendations related to assessing the possible unfairness of the AI system's outcomes on end users or subject's communities and identifying groups that might be disproportionately affected by the system's outcomes.

Pilot 4 was recommended to "test for specific target groups or problematic use cases".

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

4.2.6 Societal and Environmental Wellbeing

The pilots were all given guidance to formulate strategies that would reduce the environmental impact of their AI systems throughout their entire lifespan. Additionally, they were encouraged to participate in contests specifically designed to foster the creation of AI solutions that effectively address this challenge.

Some of the pilots were proposed to assess the environmental impact of their AI systems (pilots 2, 3, 5 and 7), to engage with impacted workers and other stakeholders (pilots 2, 6 and 7), to evaluate the work impacts of the AI system (pilots 6 and 7) and to offer training opportunities and materials for re-skilling and up-skilling measures (pilots 2, 3 and 7).

Pilot 7 got a recommendation that emphasises the importance of countering de-skilling caused by AI by providing continuous training, particularly in safety and security sensitive areas. Pilot 4 received no recommendation for this requirement.

4.2.7 Accountability

Each pilot was advised to prioritise fairness, non-negotiable values, and accountability in decision-making when utilising AI systems. They were recommended to document and thoroughly explain any conflicts or trade-offs between values to uphold these principles and their impact on people's lives.

5 Ethics Advisory Board meetings and discussions on governance and business models

During the SHAPES project, there have been so far five Ethics Advisory Board meetings (the last meeting will be held in September 2023). Discussions on SHAPES ethics and various challenges and risks related to the SHAPES ecosystem and its digital service provision are summarised in Table 17 in column 1. The mitigation strategies that are related to these challenges are reported in columns 2 and 3.

As it can be seen in Table 17, most of the challenges and their mitigation are related to SHAPES governance and business models. The challenges are linked both on the level of the provision of digital services, as well as on the level of the whole ecosystem. The ethical requirements originally defined in D8.14 in M18 cover widely the needed activities related both to organisational arrangements and to technology.

Table 17 Topics discussed in EAB meetings

Topic	Clarification	Whom the risk may concern > whose responsibility to mitigate	Ethical requirements in D8.14 and other activities needed
The terminology to be used when talking about older persons	In SHAPES, we can impact how people talk about older people in the future (e.g., older persons/people instead of elderly).	Older persons in general > society and SHAPES governance	GE47 ET1 ET2 Topic to be added in Task 3.7: Recommendations for the Adoption of the SHAPES Platform.
What is service in the context of SHAPES and its socio-technical system?	Is a digital solution a service itself, or only a tool in service provision? Should the question in the SHAPES context be: "How to create services around the digital tools?" (instead of perceiving digital solutions as services as such).	End users > service providers and SHAPES governance	This topic has been discussed in the context of the SHAPES Ethical Framework by emphasising the need for end user support services (PE1-PE7), as well as by discussing the viewpoint of care workers and their changing working practices (GE12). The topic is to be discussed more in detail in SHAPES governance model T3.4 and to be added to T3.7 recommendations—including also the terms to be used (tool vs. services vs. solution).

Digital exclusion /inclusion	Digital inclusion has several angles: social inclusion, skills (e.g., digital literacy) and e-accessibility. All these perspectives are essential.	End users > society + SHAPES governance	GE46 GE5 (indirectly) New ethical requirement “ensuring lifelong learning, including knowledge and skills needed in a digitalized world” is needed.
Social support of older people	This includes both support regarding the choice and use of services, but also human contacts and, e.g., peer support in everyday life.	Older end users > service providers + SHAPES governance	PE1-PE8 related to the support of service use. Among the SHAPES digital services there are already solutions supporting connectivity with family members and friends.
Ethics of the automatisation of care	This includes lack of human contacts but also responsibilities, liabilities, incidental findings, automated decision making, users option to switch off sensors as well as risks related to the use of intrusive technologies, e.g., facial recognition.	Older persons and caregivers as end users > SHAPES service providers and SHAPES governance	ME5-ME6 GE57 GE59 GE16 + ET21+ME7 GE38 ET3 ET15
The freedom of choice	This includes freedom of choice among various services in different service offerings, including also non-digital services.	End users > society + SHAPES governance	GE7 indirectly This freedom of choice not to use digital services is to be emphasised both in governance and business models T3.4 and T7.3 and to be added in T3.7
Older persons may not be interested in using and buying new technology	It is essential to find out how SHAPES and its digital solutions support wellbeing, diminish loneliness, etc. It is not sure that all of these solutions work and bring value.	End users > society + SHAPES governance	ME2 indirectly SHAPES pilots collect feedback from end users with the help of various wellbeing indicators. This kind of research should be done from time to time also after the project > SHAPES business and governance models T3.4 and T7.3. Getting familiar with the internet and various digital environments can also diminish the fear of using digital solutions. > Need for these kinds of learning services as part of service provision.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 857159

SHAPES customers	SHAPES platform customers are digital service providers. And the customers of digital services are older persons using the solutions. On the other hand, it is essential that in order to ensure seamless services and end user friendly customer service, it is also important to establish customer service for older persons also on the level of the platform.	End users > service providers and SHAPES governance	ME3 SHAPES governance work T3.4 and business model work in T7.3 should ensure seamless service for end users using several digital solutions.
Family caregivers are end users who may benefit from SHAPES	Persons who are not capable of giving consent may also benefit from SHAPES if their family caregivers participate. On the other hand, family caregivers may also need their own services.	Family caregivers as end users > service providers and SHAPES governance	Family caregivers of persons with cognitive impairment are involved in SHAPES pilots.
Business ethics may not be straightforward enough to put into practice holistically.	This includes also the use of external service providers as part of the SHAPES Digital Solutions.	End users + SHAPES governance + society > service providers and SHAPES governance	GE10 indirectly GE 59 SHAPES governance model and its - code of conduct - terms & conditions - self-regulation To be taken into consideration also in recommendations in T3.7.
How do we ensure that businesses and their solutions are transparent?		End users + SHAPES governance + society > service providers and SHAPES governance	GE16, GE34, GE31, ET4-5, ET9-10, ET12, ET14, ET21, PE3. SHAPES governance model T3.4 and its - code of conduct - terms & conditions - self-regulation
The tension between ethics and businesses is present in the SHAPES project.	The purpose of the SHAPES project is not to promote technology and digital services but to investigate their pros and cons critically, including ethical viewpoints. In the SHAPES project,	Business + society > SHAPES governance	

	there might be negative outcomes from the perspective of specific digital services.		
Technical platform as one outcome of SHAPES	An essential part of the SHAPES ecosystem is the technical platform enabling the SHAPES ecosystem. It is critical that the platform can be dynamic and that new services can be added into it. And that also other ecosystems may adopt the technical platform.	Local actors wanting to buy SHAPES > SHAPES business and governance	ME4 indirectly In the SHAPES project there are already open call activities. New services are evaluated from the viewpoint of SHAPES architecture, ethics etc, and added on the platform. Same kind of system will be part of the SHAPES Marketplace.
Ethical challenges related to the ecosystem-type of innovations	Ethical challenges related to single stand-alone solutions are very different from those related to ecosystems. Challenges are related not only to big data, but also to distributional ethics. - Do people have real freedom of choice to also choose services other than a certain ecosystem? - Are the services designed to be of high quality and attractive for everyone, or only to be implemented cheaply for large masses?	Older persons in general > society + SHAPES governance	GE10 + GE8 indirectly SHAPES governance model T3.4 and business model WP7, as well as T3.7 recommendations will take these into account.
Ethics approvals	Procedures regarding ethics approvals vary from country to country and this is very time consuming. There is a need to harmonise the process. In the USA there is a harmonised process. In the context of the EU, the harmonisation is challenging since each country has its own practices and	SHAPES service providers and governance > society + SHAPES governance	This will be taken into account in T3.7 policy making guidelines.

	regulations. In the background of each country there are different politics, opinions and culture. The EU does not have a formal mandate for the harmonisation.		
Time-consuming DPIA and DPO processes	There are common rules and harmonised regulation GDPR behind the DPIA process. However, the interpretation of the regulations may vary. It is always challenging to estimate the time needed for ethics and DPIA work in the project proposal phase. And it is not necessarily possible to receive enough resources for this kind of obligatory work.	Local communities adopting SHAPES + new service provides in SHAPES	GE31 ET16 This will be taken into account in T3.7 policy making guidelines.
Co-creation as a solution to many problems	We should be critical of how we organise co-creation and recruit participants. Not everyone may be interested or capable of using digital services and/or developing them. Participants co-creating should represent a variety of potential end users—and not only the lead-users. In addition, SHAPES should also collect feedback on the experiences of end users regarding the co-creation. In the SHAPES governance and business model the way the system will be developed with and for the end users is an essential part of the ecosystem. Therefore, co-creation is an important part of the	End users > SHAPES governance	GE8 The importance of R&D practices as part of the business/governance model is to be underlined.

	business/governance model. This is also a political topic: are citizens real agents of change or only objects of development (and consumers of digital solutions)?		
Secondary use of personal data	What are the possibilities for the secondary use of SHAPES personal data—both the data already collected during the SHAPES project and the data that will be collected in the future? It seems that European Health Data Space regulation may not solve the problems in wellness-type of applications (only EHR applications.) The current practices regarding the secondary use of data are fragmented at local levels. It is a risk if you rely too much on consent as the legal basis of processing. Data subjects should really understand the processing of their data for secondary use. And consent should be detailed enough to specify the purpose of the processing of data.	SHAPES service providers + governance > SHAPES governance	ET13 One solution is related to “data stewardship” and someone’s mediator role (“trustworthy middleman”) regarding secondary use. In Germany, there are several projects investigating this approach. This will then be taken into account in the data governance modelling T3.4, as well as in the final privacy and data protection deliverable D8.12 (M48). Take also into consideration in T3.7.
Data transfers between the EU and USA	There is no international agreement on the free movement of personal data between the EU and the US > Pilots have been instructed to seek devices from European manufacturers. The commission has started its work on this topic in order to	SHAPES service providers + governance > SHAPES governance	WP8 will follow up on this and updates in the final privacy and data protection deliverable D8.12.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 857159

	provide adequate decisions on the topic.		
Educational policy and care professionals' know-how on technology	We need political will to ensure that the expertise of professionals (nurses, doctors, social workers) is and remains up-to-date regarding the digitalization of the welfare sector. This is a key educational policy question and therefore also an issue related to policy making guidelines.	Society + service providers > society + SHAPES network	This will be mentioned in T3.7 recommendations.
Welfare policy and SHAPES governance & business models	Somebody has to pay for the services, and the political approach may vary regarding different healthcare systems (public services, private services, welfare mix). The key issue is to ensure the role of the public sector as the bearer of political responsibility regarding citizens' wellbeing. (>second generation human rights, EU fundamental Rights, etc.).	Society > society + SHAPES network	GE11 This will be mentioned in T3.7 recommendations and taken into account in business modelling in WP7.

6 Data management and cyber security

6.1 *SHAPES Security and Data Management Risks*

In this subchapter, we first explore SHAPES Security and Data Management risk approach (it has been presented also in D8.9) and then in chapter 6.1.2 show the findings in security and data management risk mitigation.

6.1.1 The Security and data management risks approach

This chapter builds on the first SHAPES review process and explores the security and data management risks approach and increases the promotion of a 1) table of SHAPES DMP risk assessment attributes (Table 18), 2) a table of selected cases (Table 19) for multiple case study analysis increasing the understanding of risks in the appropriate research domain (SHAPES security and data governance domain), 3) a description of higher level categories of security and data management risks in SHAPES, 4) a description of higher level categories of security and data management risks in SHAPES, 5) a data risk mitigation table for co-creation of a SHAPES security and data management risk and mitigation foundation and 6) a table of the most relevant techniques and mechanisms that can be considered for mitigation of risks in a typical SHAPES security and data management system.

Table 18 The attributes of SHAPES DMP Risk Assessment (D8.9 chapter 4.2)

Security and Data Management Risk Assessment ATTRIBUTES
DMP RISK: describing a harmful data or data management related event and its consequences, estimated in terms of severity and likelihood. Addressing the risks at the project, department and enterprise levels and increasing the awareness and monitoring of these risks. Including security, data and management views, e.g., data quality, data security and data architecture. The risks need to be considered, monitored and mitigated to reduce regulatory, financial, reputational and operational risks.
DMP RISK MANAGEMENT: coordinated activities for directing, controlling and supervision regarding risk identification and mitigation. DMP is a useful tool that helps researchers to prepare more effectively for the research process and identify potential risks. DMP also has significant pedagogical potential, and it increases collaboration activities with DMP organisations that can develop the infrastructure, services and embedded systems required to conduct research for innovations.
DMP RISK DUTY: continuous improved assessment of data management risks. The DMP risk data assessment is used to evaluate the level or degree to which data about risks is necessary for risk management. The risk duty involves analysing the form in which the risk is understood, e.g., accuracy, reliability, quality and integrity of the data concerning the risk. What data are at risk? What risk factors do data collections and archives face? How to make risks more recognised, identified and transparent?

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 857159

DMP RISK process: continuous identification, awareness and mitigation of data management risks. The OODA (observe-orient-decide-act) and PDCA (plan-do-check-act) cycles have become an important concept in risk duty, business processes, law enforcement, and strategy building, and here decision-making occurs in a recurring cycle of observe-orient-decide-act. An entity, whether an individual or an organisation, that can process this cycle quickly by observing and reacting to unfolding events more rapidly may gain advantages.
The DPIA FOCUS of SHAPES is in the operations of the protection of personal data. A Data Protection Impact Assessment (DPIA) is related to General Data Protection Regulation (GDPR) as in the SHAPES project there is a high risk to other people's personal information; the DPIA template is included for completing the assessment; ref. GDPR Article, 35, 1: with high risk to the rights and freedoms of persons, meet the legal aspects of GDPR and assess the sensitivity of data.
TRIANGULATION in the data risk and mitigation analysis processes is addressed by use of several sources of evidence. Triangulation is a powerful technique that facilitates the validation of data by cross-checking from multiple sources. There are four types of triangulations when doing assessment: data triangulation, investigator triangulation, theory triangulation and methodological triangulation, and there are countless risk factors that should be considered to ensure more safe operations, e.g., data governance flows in the cases of environmental risks, equipment risks, and people risks.

In SHAPES collective risks meetings for research design of security, risks and, mitigation activities (December 2021) a set of cases were considered as one method for increasing understanding and descriptions of critical events for the SHAPES security and data management risk approach. The research setting is integrated with shared higher education study units and outlines from the SHAPES stakeholder perspective and emphasises the SHAPES system's behaviour and responds to identified risk and mitigation as well as functionalities of resilience. In multiple case study settings, each case is represented as a sequence of simple steps, beginning with a definition of purpose (a phenomenon related approach and definition of the scope and attributes of a study), analysis by triangulation, and ending when that goal of purpose is well designed with an actualization plan. (D8.9 chapter 4.2)

The selected cases in the SHAPES data management & governance studies include attributes such as: the research domain is the SHAPES environment; the research target contributes to SHAPES data management & governance; and the Unit of Analysis (UoA) should be appropriate for multiple case studies, such as "a sample of evidence of decision-making event".

Table 19 Positioning table of cases and critical events (D8.9 Chapter 4.2)

	SHAPES DMP: Positioning TABLE of CASES and CRITICAL EVENTS
1	Decision-making with legal-ethical-moral effects.
2	Data of highly personal nature, such as sensitive and identification data.
3	Systematic monitoring: identification and decision-making support.
4	Quality check: research data, code, raw data and dissemination.
5	Data processing on a large scale, such as social intelligence (SOCINT & SOCMINT).
6	Matching or combining datasets, such as mid-range data owning.
7	Data concerning vulnerable subjects, such as risks from the perspective of humans.
8	Preventing data subjects, such as denial of a right or using a service or contract.
9	Data transfer and sharing of outside EU, such as global-local causalities and nexuses.
10	Deterrence and ransomware (phenomenon).
11	Illegal changes of data, data manipulation and vanishing of data.
12	Electronic Health Record (expanded multiple case study analysis with ENISA).
13	Remote care (expanded multiple case study analysis with ENISA).
14	Medical devices (expanded multiple case study analysis with ENISA).
15	Security measures (research continuum to ENISA and STANDARDS].

The observed security and data management risks were classified into four main categories: 1) administrative security such as security management processes; 2) personnel security; 3) physical security; and 4) information security (KATAKRI). Each of these categories consists of a multilateral classification of requirements and can be used with security level concepts that are currently being widely introduced: such as 1) the base level, 2) the increased level, and 3) the high level. The results of case studies of security and data management risks (domains) with their categorizations are included in Table 20.

Table 20 Security and data management risks (domains) (D8.9 Chapter 4.2)

DOMAINS
Administrative security (security management) risks
security policy; security action; security goals; identification process, assessing and controlling functions; organisation and responsibilities; nexus and causalities; accidents; incidents; documentation; training; awareness; knowhow; reporting; documentation; escalation.
Personnel related security risks
competence management; awareness and knowhow; suitability for the task; recruit and circulation processes; wellbeing and escalation; trust management; contracts of employment; measures; and feedback.
Physical security risks
security of area and premises; structural security (e.g., materials, windows, doors); technical systems; protection of sensitive or classified information; access rights to the rooms and domains.
Information assurance
data communications; information systems; information security; information handling and computing.

SHAPES Security and data management risks address the potential negative outcomes that can arise from insufficient or ineffective management of SHAPES data. These risks can cause concerns to reputation, financial performance, regulatory compliance, and overall ability to achieve strategic goals. The key findings of security and data management risks categories are included in Table 21.

Table 21 Security and data management risks (categories) D8.9 Chapter 4.2

CATEGORIES	
Data quality	The presence of inaccurate, incomplete, or inconsistent data. Poor data quality can lead to incorrect decisions, decreased productivity, and increased costs.
Data availability	The ability to provide timely access to data for authorised users. Data availability and access controls.
Data security	The unauthorised access, theft, or loss of sensitive or confidential data. Data breaches can result in significant financial and reputational damage, legal liability, and regulatory penalties.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

Data privacy	The ability to comply with data privacy regulations and protect personal information. Privacy impact assessments and compliance audits.
Data loss	This risk addresses the accidental or intentional loss of data, which can result in significant financial and reputational damage.
Backup and recovery Resilience	This risk refers to the failure to regularly back up data and implement effective recovery procedures. Inadequate backup and recovery procedures can result in significant data loss and downtime.

6.1.2 The findings of security and data management risk mitigation issues

The findings of security and data management risk mitigation issues are described in Table 22.

Table 22 Security and Data Management Risk Mitigation Mechanisms

MITIGATION MECHANISMS	
Mitigation procedures	Specific threat and mitigation models and methodologies in SHAPES.
Nexus management	Understanding and taking into account mutual impacts and causalities.
Response solutions	Restore and retrieve functionalities; backup version management including restore with cleaning and finding of possible damaged files from earlier backup or achieve versions.
Federated coordination	Cooperation such as security operations centres and cyber ranges; incident response across federated organisations (SIRTFI).
Resilience	Prevention and recovery capabilities; sense of resilience as alternative paths for recovery; applied resilience engineering.
Information sharing environment	Database of live pages that can manage mitigation and response information (e.g., wiki dedicated pages); using FAIR Digital Objects and Encapsulation.
Reference library	A globally accessible knowledge base of adversary tactics and techniques based on real-world observations, e.g., MITRE ATT&CK.

Mitigation of risks in the SHAPES environment and in a typical data management system requires a design of a novel asset management framework that captures the input and analysis required to ensure the resilience, prevention, preparedness, and mitigation of risk under extreme events as well as normal operating conditions. Here, the case study analysis is addressed with the term “mitigation” as the unit of analysis that considers “mitigation from the perspective of functionalities & functions in the use cases (described in the position Table 22 above) by using security concepts and classes of technologies that can be employed to prevent a harmful technique from being successfully executed. Table 23 describes the most relevant techniques and mechanisms that can be considered for the mitigation of risks in a typical SHAPES security and data management system.

Table 23 Findings of key mitigation activities for risks in a typical data management system environment

FINDINGS OF KEY MITIGATION ACTIVITIES	
Login & logout	Configure use of account information, login attempt and logouts, specific login times, use log files for selected data records.
Domain control	Configure domain controls: to prevent use of certain harmful techniques, use a digital identity functionality.
Detect malicious software	Use of recognition: signatures, heuristics, antivirus, and antimalware functionalities.
Developer responsibility	Guidance or training given to developers of applications to avoid introducing security weaknesses.
Application isolation	Restrict execution of code to a virtual environment (e.g., use of private network).
Using of audits	Perform audits or scans of systems, permissions and configurations to identify potential weaknesses.
Secure system bootstrap	Use secure methods to boot a system and verify the integrity of the operating system and loading mechanisms.
Code signing	Enforce binary and application integrity with digital signature verification to prevent untrusted code from executing.
Credential access protection	Use capabilities to prevent illegal credential access, e.g., including blocking forms of credential dumping.
Data backup	Take and store data backups from systems and critical servers; keep copy of backups in separate storage from the corporate network.
Corrupted backup data	Keeping multiple backup versions; using anti-ransomware and cleaning software; intercepting corrupted data and software before backup process; and isolated restore and cleaning process.
Data activity monitoring	Monitoring datafiles and databases transactions, including both data definition and data manipulation transactions.

Encrypt sensitive information	Protect sensitive information with appropriate level of encryption.
Filter network traffic	Use network appliances to filter ingress or egress traffic and perform protocol-based filtering; configure management software on local network.
Control of installations	Control installing or using unapproved hardware or software, including such as USB devices and unapproved software.
Authentication	Use multi-factor and strong authentication.
Network segmentation	Isolate critical systems, functions, or resources; using of physical and logical segmentation to prevent access to potentially sensitive systems and information.
Policies	Secure password policies for accounts; data reservation and retention policies; backup and achieve policies; access control policy; duties policy.
Privileged mode and account management	Manage the creation, modification, use, and permissions associated to privileged accounts and modes; reboot control and system management.
Threat intelligence	Use of threat intelligence programs for generation of threat intelligence information to mitigate risks.
Update software	Perform regular software updates to mitigate emergent risks.
Account management	Manage and control of the creation, modification, use, and permissions associated with accounts.
Training and responsibility	Training of users to be aware of access or manipulation attempts and for reduction of social risks.
Vulnerability scanning	Use of vulnerability scanning for finding and recognizing potential software vulnerabilities.

6.2 Cybersecurity risks

Cybersecurity ethics is a multidisciplinary practice that includes influences from different fields of study, such as medical ethics, military ethics, legal ethics, and media ethics. Therefore, cybersecurity ethics can be considered as professional ethics that provide in-depth and specific knowledge to actors with certain characteristics (Manjikian 2018).

6.2.1 Literature analysis (D8.14, Chapters 6.2.1 & 6.2.2)

According to Van de Poel (2020), four value clusters should be taken into account when deciding on cybersecurity measures:

1) The *security cluster* (individual security, national resilience, and information security) protects against all kinds of harm and responds to morally problematic situations where harm occurs, from data breaches and loss of data integrity to cybercrime and cyberwarfare.

2) The *privacy cluster* (privacy, moral autonomy, human dignity, identity, personhood, liberty, anonymity, and confidentiality) highlights that we should treat others with dignity, we should respect people's moral autonomy, we should not store or share personal information without people's informed consent, and we should not use people or information about them as a means to an end. The moral problems of these values are the secret collection of large personal data for cybersecurity purposes or the unauthorised transfer of personal data to a third party.

3) The *fairness cluster* (justice, fairness, equality, accessibility, freedom from bias, non-discrimination, democracy, and the protection of civil liberties) emphasises that cybersecurity threats and measures to avoid them do not treat everyone equally and are morally unfair. A moral problem is that cyber security threats or actions to increase cyber security can undermine democracy, civil rights, and freedoms. People should be treated fairly and equally, and democratic and civil rights must be cherished.

4) The *accountability cluster* (transparency, openness, and explainability) means that if governments implement cybersecurity measures that harm citizens and require weighing multiple conflicting substantive values such as security, privacy, and justice, accountability as a more procedural value is particularly important.

Domain-specific ethical principles and values vary in each domain, and technical goals can be different from application to application. They relate to instrumental or technical values related to the proper functioning of applications, such as efficiency, ease of use, understandability, data availability, reliability, compatibility, and connectivity. Technical values are morally important because they enable the achievement of moral values (van de Poel, 2020).

6.2.2 Desiderata of ICT in health care and the instrumental role of cybersecurity

According to Weber and Kleine (2020, 143-145), healthcare (H&C) ICT systems have four main tasks:

1. Improving the quality and efficiency of services. H&C ICT systems handle information management, which enhances the H&C system and reduces costs.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

Qualitative improvements mean, for example, new care services or processes that have better health-related outcomes.

2. Protecting confidentiality. Processing patient data creates a moral challenge in terms of quality and efficiency versus privacy and confidentiality—both being important goals in H&C. Privacy is often seen as a prerequisite for patients' autonomy, and therefore privacy is related to the principle of autonomy. Privacy and confidentiality are also the basis of trust between patients and healthcare professionals.
3. Enhancing usability. Usability can be seen as the degree of effectiveness, efficiency, and satisfaction with which users of a system can realize their intended task. Users include patients, medical staff and/or administrators, which have different degrees of ICT competencies, depending on personal attitudes and socio-demographic variables.
4. Protecting patients' safety (= reducing health risks). Safety, quality, efficiency and usability are interrelated, but on the other hand, safety measures might reduce the efficiency and usability of services and therefore quality.

The instrumental role of cybersecurity in H&C is to protect against threats to (1) information, (2) information systems, and (3) medical devices (Loi, et al., 2019).

6.2.3 Ethical decision-making risks related to cybersecurity

Figure 14 combines the ethical dimensions related to cybersecurity. The previous chapter presented the values that guide technology and data processing. From the legislative side, important regulations to take into account are the general data protection regulations, medical device regulations, and EU fundamental rights. The main values that guide the activities are bioethics and ethics of care.

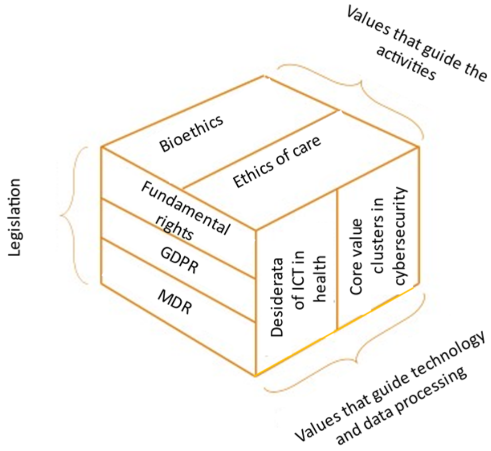

Values that guide the activities
Bioethics
Ethics of care
Legislation
Fundamental rights
GDPR
MDR
Desiderata of ICT in health
Core value clusters in cybersecurity
Values that guide technology and data processing

Figure 14 Dimensions of ethical decision-making in health technologies and services

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

Cybersecurity and healthcare professionals should consider ethics as part of their profession and understand the ethical significance of their profession. An ethical cyber security professional uses his skills both to build a better product or service and to strive towards a better world (Manjikian 2018). Conflicts within the core values of cyber security and between the core values of cyber security and other values, for example, those related to bioethics and ethics of care, make compliance with ethical values complicated. Excessive investment in cyber security, for example by increasing or restricting the use of the internet, contradicts privacy and freedom. (Christen, et al. 2020).

Table 24 is a simplified matrix of simultaneous consideration of different values. Its rows consist of the ethical values that guide healthcare operations (bioethics + ethics of care), and the columns consist of values that guide technology and data processing (core tasks of healthcare information technology + cyber security value clusters). The table has a total of 56 cells, each of which represents one pair of values.

Table 24 Simplified matrix for considering ethical value pairs

		Desiderata of ICT in H&C				**Core value clusters in cybersecurity**			
		Efficiency and quality of service	Privacy of information and confidentiality of communications	Usability of services	Safety	Security	Privacy	Fairness	Accountability
Bioethics	Autonomy	(1.1)	(1.2)	(1.3)	(1.4)	(1.5)	(1.6)	(1.7)	(1.8)
	Nonmalefience	(2.1)	(2.2)	(2.3)	(2.4)	(2.5)	(2.6)	(2.7)	(2.8)
	Beneficence	(3.1)	(3.2)	(3.3)	(3.4)	(3.5)	(3.6)	(3.7)	(3.8)
	Justice	(4.1)	(4.2)	(4.3)	(4.4)	(4.5)	(4.6)	(4.7)	(4.8)
Ethics of care	Empathy	(5.1)	(5.2)	(5.3)	(5.4)	(5.5)	(5.6)	(5.7)	(5.8)
	Relationships	(6.1)	(6.2)	(6.3)	(6.4)	(6.5)	(6.6)	(6.7)	(6.8)
	Uniqueness of the case	(7.1)	(7.2)	(7.3)	(7.4)	(7.5)	(7.6)	(7.7)	(7.8)

Next, there is a look at some of the value pairs in Table 24 as examples, i.e. what does favouring one value at the expense of the other mean in terms of cyber security?

(3.1) Improving the quality of services increases costs, which is at odds with benefit maximisation, which also considers cost efficiency.

(3.2) The maximum possible sharing of patient data and other health-related data enables medical progress but may compromise privacy.

(3.5) If the pursuit of benefit is emphasised on the basis of cost efficiency and the price of the service, it can lead to a weakening of the security of the services.

(1.5) Strict access control created to improve data security can prevent the patient from managing his own data, and thus he can have little influence on decision-making. In this case, the patient's autonomy can end up being completely ignored.

(1.3) To improve usability, the user can only be given a few options. Autonomy decreases when the number of options to choose from decreases.

(2.5) Information security procedures can be so demanding that only well-informed users can access the full potential of the services.

(4.5) If the encryption of a pacemaker's wireless data transmission is improved for example (data security), the increased need for computing power increases energy consumption. This can lead to battery replacement requiring surgery.

Table 24 is suitable for evaluating the dependencies and contradictions of the values that guide operations and technology and data processing. However, even within the same framework, there are conflicting values, of which the following are some examples:

1. Usability vs. information security: Information security can be a disadvantage to usability and too easy usability a threat to information security, but too difficult usability is also a threat to information security because if the user does not know how to use a certain service, he can break or crash the device or service (Loi, Christen, Kleine & Weber, 2019). One example of improving information security is authentication requiring two or more parts, where the information security of the service increases, but the several steps slow down the use of the service. Especially in services that a person uses several times a day, this slowdown reduces usability.
2. Privacy is opposite in value to the efficiency and quality of services. In the quality and efficiency of services, one key factor for improving services is sharing information with others and thereby finding new solutions.

6.3 Mitigation possibilities

Handling cybersecurity involves a lot of ethical decision-making and ethical risks. Value conflicts between the values that guide the activities of medicine and nursing sciences, and the values that guide health technology and data processing make decision-making difficult. The best result can only be reached by making compromises between values. Which value do we want and are able to be flexible with so that we can invest more in the second value? There is not just one right answer here and it requires ethical reflection and understanding of one's own value base and putting into practice which values one wants to give up and which to emphasise. Individual and cultural differences must also be taken into account. What would mean the most desirable outcome for us, does not necessarily mean the same in another society or in another person's opinion at all. In addition, the weights of conflicting values are very situational: during a life-threatening accident or illness, few first-aid patients are primarily concerned about their privacy.

The matrix (Table 24) contains 56 (7 x 8) ethical value pairs. Since the trade-offs between these are individual and situation-related, a Fuzzy Multi-Criteria Decision-Making (FMCDM) approach could be suitable as a solution. The technology to build an ethical decision-making support system exists, but more interdisciplinary research is needed to define the relative importance of the criteria of the FMCDM decision matrix, to build a prototype, and to test its functionality in a health technology service.

7 Conclusion

This second SHAPES ethics and privacy risk management deliverable (D8.10) is mainly composed of inputs coming from pilots' ethics risk workshops, AI assessments, and DPIAs. In addition, themes, which are especially relevant from the SHAPES governance and business viewpoint in the wide production phase beyond the pilots, were also investigated and discussed in SHAPES Ethics Advisory Board meetings.

The original ethical requirements in D8.14 (based especially on EU fundamental Rights, the UN Convention on Rights of Persons with Disabilities, bioethics, ethics of care, human capabilities, general data protection regulation, ALTAI's Trustworthy AI assessment list and the UN Sustainable Development goals) widely cover the identified risks and mitigation activities. Some new ethical viewpoints also emerged during the discussions both with pilots and with the EAB and they are updated in the final list of ethical requirements (see Appendix 1). By taking into account these ethical requirements and aspects, many of the identified risks can be seen as opportunities to provide value. For example, ethical requirements stemming from the UN Convention on the Rights of Persons with Disabilities regarding, e.g., supported decision making and universal design make the digital inclusion of persons with diminishing capacities easier.

In Table 25, there is a summary of the categories of ethics risks and opportunities identified during the first half of the project (see D8.9) in the second column, and corresponding categories formulated during the second of the project (this deliverable). As it can be seen in the columns, they are complementing each other and providing a summary of the ethics risks and opportunities identified and managed during the SHAPES project.

Table 25 Summary of the ethics risks and opportunities of SHAPES

Categories and contents related to risk mitigation in this deliverable D8.10	Categories in the first ethics and privacy risk assessment D8.9
Independence and autonomy of older adults	
Provide end users clear and accessible information about digital services, enabling them to make informed decisions. Respect the freedom to choose whether to use digital services or opt for alternative options, without coercion or pressure. Ensure the right to disconnect systems when desired.	Informed consent and advocacy mandate End-users' capacity/ willingness to use technology Autonomy and freedom of choice

Human care in the context of digital services	
Ensure that the caregiver-caretaker relationship will not disappear or diminish too much. Understand the need for the social support of older people. Respect guardianship of caregiver's interest. Provide face-to-face care-providing chains, if necessary. Understand the interaction with people as an important part of the digital solution.	Holistic conception of wellbeing Human contacts and interpersonal networks
Care providers viewpoint	
Pay attention to the workload of care providers' and family caregivers' everyday life. Also consider family caregivers as key end users who may benefit from SHAPES. Ensure that the expertise of professionals (nurses, doctors, social workers) remains up-to-date regarding the digitalization of the welfare sector. This is a key educational policy question and therefore also an issue related to policy making guidelines.	Care workers' wellbeing and work Family caregivers' wellbeing
Equity and digital inclusion	
Understand that digital inclusion has several angles: social inclusion, skills (e.g., digital literacy) and e-accessibility. All these perspectives are essential to be promoted. Consider cultural, gender and language factors when planning and providing services. Ensure fair funding models for services also for those who are less well-off. Consider the terminology to be used when talking about older persons. Use non-stigmatizing language.	Different cultures and backgrounds of people Self-image and non-stigmatization Digital inclusion
Data Protection, Cyber Security and Data Management	
Ensure full compliance with GDPR, including data minimisation, well-designed consent procedures and processes for data subjects to exercise their rights (access to information, right to be forgotten etc). Provide end-user training. It is important that older people understand and accept where and how information is collected and with whom it is shared. Careful and detailed explanation why the data is being collected and how the data minimisation has been applied. Set up a human-contact point for participant concerns. Carefully evaluate the benefits and harms to health and quality of life, such as reduced privacy: which causes less harm and more benefits? Set up monitoring systems and incidence reporting protocols. Upon incident detection, the incident response team will assess the event consequences towards designing and deploying the necessary technical and organisational control measures. Establish a data management framework which captures the input and analysis required to ensure the resilience, prevention, preparedness, and mitigation of risk under extreme events as well as normal operating conditions.	Privacy and data protection Data management Cybersecurity

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

Follow up the evolving regulations, including secondary use of personal data and Data transfers between the EU and USA.	
Trustworthy Artificial Intelligence (adopted from ALTAI 2021)	
Ensure the following: • Human agency and oversight • Ensure technical robustness and safety • Privacy and data governance • Transparency • Diversity, non-discrimination and fairness • Societal and environmental wellbeing • Accountability	Big data and AI Incidental findings
Business and access to sustainable services	
Remember the role of the public sector as the bearer of political responsibility regarding citizens' wellbeing. Ensure public supervision of services and their development. Apply/develop certification for digital solutions. Be aware of the various challenges related to automatised care. This includes lack of human contacts but also responsibilities, liabilities, incidental findings, automated decision making, users' option to switch off sensors as well as risks related to the use of intrusive technologies, e.g., facial recognition. Remember that digital tools alone are not services yet. Various support services are needed around these tools in order to transfer them as services. Take into use Codes of Conducts to ensure joint understanding on the value base of SHAPES services and their provision. From time to time, find out how SHAPES and its digital solutions support wellbeing, diminish loneliness, etc. It is not sure that all these solutions work and bring value. SHAPES platform customers are digital service providers, and the customers of digital services are older persons using the solution. However, in order to ensure seamless services and end user friendly customer service, it is also important to establish customer service for older persons also on the level of the platform.	Responsibilities and liabilities Quality of services Social, economic and environmental sustainability
Co-creation with and for the end-users and other stakeholders	
In the SHAPES governance and business model the way the system will be developed with and for the end users is an essential part of the ecosystem. Therefore, co-creation is an important part of the business/governance model. This is also a political topic: are citizens real agents of change or only objects of development (and consumers of digital solutions)? Apply Human-centric design, also including utilisation of the knowledge of experienced experts. Carefully design the process, including background research to understand the lifeworld of older adults and family caregivers. Be critical of how to organise co-creation and recruit participants. Not everyone may be interested or capable of	Challenges with project -based development

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

using digital services and/or developing them. Participants co-creating should represent a variety of potential end users— and not only the lead-users.	

The outputs of this deliverable provide essential inputs for the design of the final SHAPES governance and business models in WP3 and WP7 with their different layers, responsibilities, and functionalities, including codes of conduct. In addition, several ethical risks and their mitigation can be formulated as SHAPES recommendations in WP3.

8 Ethical requirement check

The focus of this compliance check is on the ethical requirements defined in D8.4 that have an impact on the SHAPES solution (technology and related digital services, user processes and support, governance-, business- and ecosystem models). In the left column are the ethical issues identified and discussed in D8.4 (corresponding D8.4 subsection in parenthesis). For each deliverable, report on how these requirements have been taken into account. If the requirement is not relevant to the deliverable, enter N / A in the right-hand column.

Ethical issue (corresponding number of D8.4 subsection in parenthesis)	How we have taken this into account in this deliverable (if relevant)
Fundamental Rights (3.1)	See chapter 3.1.1
Biomedical Ethics and Ethics of Care (3.2)	See chapter 3.1.4
CRPD and supported decision-making (3.3)	See chapter 3.1.2
Capabilities approach (3.4)	See chapter 3.1.3
Sustainable Development and CSR (4.1)	See chapter 3.3.2
Customer logic approach (4.2)	See chapter 3.3.2
Artificial intelligence (4.3)	See chapter 4
Digital transformation (4.4)	See chapter 2
Privacy and data protection (5)	See chapter 2
Cyber security and resilience (6)	See chapter 6
Digital inclusion (7.1)	See chapter 3.4.1
The moral division of labour (7.2)	See chapter 3.4
Care givers and welfare technology (7.3)	See chapter 3.4
Movement of caregivers across Europe (7.4)	See chapter 3.4

Comments: ____

References

American Psychological Association. (2010). Publication manual of the American Psychological Association (6th ed.). Washington, DC: Author

Christen, M., Gordijn, B. and Loi, M. (2020a). The Ethics of Cybersecurity, Cham: Springer Nature, 2020.

Christen, M., Gordijn, B. and Loi, M. (2020b). Introduction, in The Ethics of Cybersecurity, Cham, Springer, 2020, pp. 1-8.

Christen, M., Loi, M. and Kleine, N. (2018). Cybersecurity in health – disentangling value tensions, in Ethicomp 2018, Sopot/Poland, 2018.

Cormi, C., Petit, M., Auclair, J., Bagaragaza, E., Colomnet, I. & Sanchez, S. (2021). Building a telepalliative care strategy in nursing homes: a qualitative study with mobile palliative care teams. BMC Palliat Care (2021) 20:156. Accessed 29 November 2021. https://doi.org/10.1186/s12904-021-00864-6

Custers et al. 2018 in North-Samardzic (2020). Biometric Technology and Ethics: Beyond Security Applications. J Bus Ethics 167, 433–450 (2020). Accessed 21 November 2021. https://doi.org/10.1007/s10551-019-04143-6

Loi, M., Christen, M., Kleine, N. and Weber, K. (2019). Cybersecurity in health– disentangling value tensions. Journal of Information, Communication and Ethics in Society, vol. 17, no. 2, pp. 229-245, 2019.

Manjikian, M. (2018). Cybersecurity Ethics - An Introduction., New York: Routledge, van de Poel, I. (2020). Core Values and Value Conflicts, in M. Christen et al. (eds.), The Ethics of Cybersecurity., Cham, Springer, 2020, pp. 45-72.

MacLachlan, M., McVeigh, J., Cooke, M., Ferri, D., Holloway, C., Austin, V., & Javadi, D. (2018). Intersections Between Systems Thinking and Market Shaping for Assistive Technology: The SMART (Systems-Market for Assistive and Related Technologies) Thinking Matrix. International Journal of Environmental Research and Public Health, 15(12), 2627. doi:10.3390/ijerph15122627

Rajamäki, J., Gioulekas, F., Rocha, P.A.L., Garcia, X.d.T., Ofem, P. & Tyni, J. ALTAI Tool for Assessing AI-Based Technologies: Lessons Learned and Recommendations from SHAPES Pilots. *Healthcare* 2023, *11*, 1454. https://doi.org/10.3390/healthcare11101454

Weber, K. & Kleine, N. (2020). Cybersecurity in Health Care, in The Ethics of Cybersecurity, The International Library of Ethics, Law and Technology 21, Cham, Springer, 2020, pp. 139-156.

Annex 1: Ethical requirements

No	Requirement	Importance	More information in D8.14 section	Old numbers in D8.14
GE1 **(GE= general ethical requirement for the R&D work)**	Maximise the level of fundamental rights of older persons and of care givers that SHAPES and its digital services can promote. Ensure they do not violate any fundamental rights of older persons and/or other stakeholders (e.g., non-discrimination, dignity, integrity and privacy when having robots, web-cameras at home),	Essential/Mandatory	Rights, Disabilities, AI Ethics, Privacy & DP, Lifelong Learning	GE1, GE2
GE1	Be aware of the four biomedical principles and perspectives of care ethics. Apply and promote those within SHAPES (justice, beneficence, non-maleficence autonomy, empathy, relationships, uniqueness).	Essential/Mandatory	Bioethics, AI ethics, Cybersecurity	GE4, GE4
GE3	Adopt holistic approach to wellbeing and good life. Maximise the level of human capabilities of older persons and caregivers that SHAPES and its digital services can promote. Ensure that SHAPES is not detrimental to any human capabilities of older people and/or other stakeholders. Pay attention especially to those who are weaker of with disabilities.	Essential/Mandatory	Disabilities, Capabilities, Lifelong Learning	GE5, GE6, updated requirement
GE4	Digital inclusion, acknowledge: -Heterogeneity of (older) persons that materialise in the diversity of how persons adopt and use digital devices -Barriers and facilitators of (older) persons' usage of digital devices (perception of usefulness, user requirements, self-efficacy, sense of self, privacy and confidentiality, cost). -Diversity and complexity of ageing and incorporate that gained understanding into the design process of health technology devices, including the realistic assessment or their usability.	Essential	Disabilities, Digital inclusion, Lifelong learning	GE48, GE49, GE50
GE5	Remember that technology and digital solutions are only tools around which the service will be built, including also needed support services.	Essential	Customer logic	new requirement
GE6	Consider that the public sector, as part of the SHAPES ecosystem, plays a role as a bearer of political responsibility for ensuring the wellbeing of older persons. In addition to the collaboration in governance and service development, this collaboration may be related to e.g. service supervision and certificates.	Essential/Mandatory	Rights, Capabilities, Sustainable development	GE11, updated requirement
GE7	Note that the participation of older persons in the development and governance of SHAPES can in itself be seen as a service that supports a person's human capabilities. Ensure that end-users have real power and impact in service development. Consider working methods and tools in the end-user collaboration so that they support a person's capabilities and ensure that essential information on end-users' needs is captured.	Essential	Capabilities, Disabilities, Inclusion, Customer logic, Division of Labour, Lifelong learning	GE8, GE9
GE8	Develop and choose solutions that offer users different options to act according to their own choice and practical reasoning. Be open to innovations that may not presuppose commercial commodities of digital tools.	Essential	Capabilities, Division of labour	GE7, updated requirement
GE9	Investigate and collect user feedback related to services that may be considered intrusive (for example facial recognition), risky for autonomy or for depersonalisation or for sense of security (for example robots) or associated with a surveillance type of services without one's own control (sensors at home). Find out how end-users experience the processing of their own personal data.	Essential	Rights, Ethics of Care, Capabilities	GE57

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

GE10	Be aware of the importance and challenges with the terminology regarding older persons, also in your own language as well as the diversity of older persons as a group. Use non-stigmatising language.	Essential	Rights, Disabilities, Terminology	GE47
GE11	Apply Universal Design and Design for all – approaches.	Essential	Rights, Disabilities, Digital inclusion, Lifelong learning	GE58
GE12	Respect the role of caregivers as guardians who understand the lifeworld of the end-user.	Essential	Careworkers, Ethics of Care, Bioethics	new requirement
GE13	Be aware that the use of various digital solutions has an impact on the workload of caregivers but also their work displacement. Investigate the improvement and provide training.	Essential	Rights, Caregivers, Sustainable development	GE 12, GE13
GE14	Ensure SHAPES AI solutions: -Human agency and oversight -Technical robustness & safety -Privacy and data governance -Transparency -Diversity, non-discrimination -Societal and environmental wellbeing -Accountability	Mandatory	AI Ethics, Rights, Capabilities, Sustainable development, Lifelong learning	GE16-GE22
GE15	Ensure Data subject rights: right of access, right to rectification, right to be forgotten, right to restriction, information to 3rd parties, right to data portability, right to object	Mandatory	Privacy & DP	GE24-GE30
GE16	Privacy by design and by default: ensure data protection is taken into account when start planning for new services or processes. Adopt a "privacy first" approach.	Mandatory	Privacy & DP	GE39
GE17	Conduct DPIA and ensure that the following data protection principles are embedded in the DPIA: lawfulness, fairness, transparency, integrity and confidentiality	Mandatory	Privacy & DP, Data processing description and DPIA (appendix)	GE31-GE36, GE40, GE46
GE18	Personal data breach: ensure that data controllers and processors have a process for handling personal data breaches, including communication to the data subject and to the supervisory authority.	Mandatory	Privacy & DP	GE41
GE19	Technical and organisational security measures: identify and document who needs to have access to personal data.	Mandatory	Privacy & DP	GE42
GE20	Ensure that privacy and data protection related legal documents are in place (for example NDAs and data processing agreements).	Mandatory	Privacy & DP	GE45
GE21	Implement and update Security and Resilience Management Plan that covers all four event management cycles (plan/prepare, absorb, recovery, adapt) and interdependencies with other systems.	Essential/Mandatory	Cybersecurity	GE55
GE22	Ensure that legal frameworks on local and EU-level related to the SHAPES Integrated Care Platform are taken into account. Follow up also policy papers.	Mandatory	Legal framework (see appendix)	GE59
ET1 **(ET= ethical requirement for the technology)**	Ensure equal and non-discriminatory access to technology and its support services by using well-designed user interfaces, instructions and authentication.	Essential	Rights	ET10
ET2	Consider language differences and cultural diversity of users; for example, create avatars that represent different genders and cultures and let the user choose what to use. Use gender appropriate language.	Essential	Rights, Capabilities	ET2, updated requirement
ET3	Create functionalities for the end-user to switch off/on various sensors and services whenever she/he want to do it.	Mandatory	Rights	ET3
ET4	Data subject rights: right of access – provide a self-service portal where the data subject can get access to his/her data.	Desirable	Privacy & DP	ET4

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

ET5	Data subject rights: right to rectification – ensure that the data can be corrected in all places (incl. storage).	Mandatory	Privacy & DP	ET57
ET6	Data subject rights: right to be forgotten – build capabilities for deleting personal data.	Mandatory	Privacy & DP	ET6
ET7	Data subject rights: right to restriction – build a capability for restricting data processing.	Mandatory	Privacy & DP	ET7
ET8	Data subject rights: information provided to third parties – create a functionality to get information about the third parties to whom data has been disclosed as part of robust data mapping and flows.	Mandatory	Privacy & DP	ET8
ET9	Data subject rights: right to data portability – create a capability to transmit data to the data subject/third party in a structured, commonly used and machine-readable format.	Mandatory	Privacy & DP	ET9
ET10	Data subject rights: right to object: 1) ensure that the information about automated decision-making can be given to the user (the data subject) before the process starts; 2) create the capability to prevent the data subject's data to be part of profiling if a data subject has objected to profiling.	Mandatory	Privacy & DP	ET10
ET11	Data protection principles: storage minimisation – ensure that there are technical capabilities to erase or anonymise personal data after the relevant data retention period. Ensure that data will be removed from all systems. Define automated functions if this is possible.	Mandatory	Privacy & DP	ET11
ET12	Data protection principles: accuracy – ensure that the source of the data is recorded.	Mandatory	Privacy & DP	ET12
ET13	Legal basis: a) ensure that there are sufficient capabilities for asking consent as part of the service and that the consent is documented properly (obligatory); b) build up a repository where consents can be collected centrally (optional – to be defined if it brings value to SHAPES).	Mandatory	Privacy & DP	ET13
ET14	Create traceability capabilities for personal data; data mapping/data flows.	Mandatory	Privacy & DP	ET14
ET15	Automated decision-making: Ensure that there's a capability to re-direct the decision to a manual process.	Mandatory	Privacy & DP	ET15
ET16	Privacy by design and by default: implement needed privacy enhancing technologies.	Mandatory	Privacy & DP	ET16
ET17	Personal data breach: create capabilities to identify potential personal data breaches	Mandatory	Privacy & DP	ET18
ET18	Technical and organisational security measures: ensure that users' access can be limited to certain categories of personal data and the need to restrict access to certain data is taken into consideration in SHAPES architecture.	Mandatory	Privacy & DP	ET19
ET19	Keep logs for personal data (who has seen/modified personal data and when).	Mandatory	Privacy & DP	ET20
ET20	Deploy the functionalities related to the trustworthy AI guidelines.	Mandatory	AI Ethics	ET21
ET21	Utilise the AI solutions also to provide self-diagnosis of the SHAPES's security and other issues.	Optional	AI Ethics	ET22
ET22	Deploy the technical functionalities related to security & cybersecurity	Mandatory	Cybersecurity	ET23, GE52
ET23	Ensure that penetration testing is undertaken for software solutions.	Mandatory	Cybersecurity, AI Ethics	GE56

ET24	Follow the WCAG 2.1. Standards and Universal Design principles in designing and implementing process. Perform formative, summative, and continuous evaluations. Test throughout the project lifecycle and any time new content is added or code is updated.	Mandatory	Persons with disabilities	ET24
ET25	Ensure the platform usage by using assistive technology (screen magnifiers, text-to-speech, colour combinations with high contrast etc.)	Essential	Persons with disabilities	ET26
PE1 **(PE= ethical requirement for user processes)**	Provide a process for the implementation of services for single end-users (older persons) + and for the assessment of the suitability of the services from time to time (including a process to assess the digital literacy of the end-user and adapt the services according to end-user needs and capabilities). The process should include more time to discuss choices or have an advocate regarding important appointments in order to make notes and help the person understand or remember choices.	Essential	Capabilities, Customer logic, Lifelong learning	PE1
PE2	Provide a detailed process to determine if the older person is able to decide on accessing the services and secondly if she/he is able to give informed consent and re-consent for the collection of the information. In that work take into consideration also local regulations.	Mandatory	Persons with disabilities, Privacy & DP	PE2
PE3	Provide for the end-user (older persons) plain and understandable language materials, instructions, information in visual form (including information on each service and how it operates and what data it collects.)	Essential/Mandatory	Persons with disabilities, Lifelong learning	PE3
PE4	Provide general training on data protection and cybersecurity to end-users (older persons, caregivers, researchers) in order to enhance their understanding on digital environments.	Essential/Mandatory	Privacy & DP, Cyber-security, Lifelong learning	PE4 updated requirement
PE5	Provide help contacts or communication aids for SHAPES users, including possibility to communicate with humans, not only chatbots.	Essential	Persons with disabilities	PE8 updated requirement
PE6	Provide support and process for executing data subject rights in SHAPES.	Mandatory	Privacy & DP	PE6
PE7	Provide processes and guidelines regarding the incidental findings when using or analysing SHAPES data.	Mandatory	AI ethics, Bioethics	ME6
PE8	Carefully design the contents of the consents and information to be provided about the data processing, including explanation why sensitive data is necessary to process.	Mandatory	Privacy & DP	new requirement
ME1	Create a process to ensure that members of the SHAPES Integrated Care Platform (during the open calls and after the project) have the capabilities to comply with mandatory ethical requirements.	Mandatory	all the chapters	ME4
ME2	Deploy responsibilities /liability regarding the SHAPES and each of its various services (for example if something goes wrong, if the quality of data is poor, false positive & false negative situations). This includes processes related to the personal safety solution that require organisational arrangements.	Mandatory	Rights, AI Ethics, Legal framework (appendix)	ME5
ME3	Consider Corporate Social Responsibility, Sustainable Development Goals and ISO 2600 in order to optimise the value SHAPES can bring to society. Work towards both the economic, social and environmental sustainability of SHAPES.	Essential	Sustainable development	GE10
ME4	Adopt customer logic in the building and expansion of the SHAPES Integrated Care Platform and its business governance. Pay attention to the fact that even the most marginalised should be able to use SHAPES.	Essential	Rights, Capabilities, Disabilities, Customer logic, Sustainable development	ME3, GE10

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

ME5	Update the SHAPES Code of Conduct that outlines the value base and key principles of the SHAPES (to be utilised especially after the SHAPES project itself has ended and the realisation begins).	Mandatory/essential	Code of conduct	ME1
ME6	Provide periodical audits and process to conduct Societal Impact Assessment (SIA) and Fundamental Rights Impact Assessment (FRIA) of the SHAPES Integrated Care Platform (and especially related to AI) on a regular basis, including the compliance with regulatory frameworks and recommendations.	Essential/Mandatory	Sustainable development, AI Ethics	ME2
ME7	Establish AI governance and management for SHAPES.	Mandatory/Essential	AI Ethics	ME7
ME8	Establish privacy and data protection governance model for SHAPES - Roles and responsibilities - Data subject rights - DPIAs - Privacy information - Privacy policy	Mandatory	Privacy & DP	ME8ME9, ME11, GE 40, GE46
ME9	Create and implement the cybersecurity and resilience management of the SHAPES Integrated Care Platform	Mandatory/Essential	Cybersecurity	ME14
ME10	Update and publish data protection and cybersecurity policies + provide accessibility statement	Mandatory	Privacy & DP, Cyber-security, Disabilities	ME15, GE23
ME11	Be aware of skills and specific competences needed for the care givers using the SHAPES services and provide training materials.	Essential	Careworkers	PE7