SHAPES

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

D8.11 – Privacy and Data Protection Legislation in SHAPES

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	Juhamatti Etuaro (LAUREA)
Contributors	Nina Alapuranen (LAUREA), Sari Sarlio-Siintola (LAUREA), Rauno Pirinen (LAUREA), Nicola Goodfellow (NHSCT), Michael Scott (NHSCT), Artur Krukowski (ICOM)
Peer reviewers	Dewar Finlay (ULS), Susan Quinn (ULS), Shirley Davey (ULS), Meftah Ghrissi (KOM)
Version	V1.0
Due date	M24 – 31/10/2021
Submission date	26/10/2021
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	30/06/2021	Nina Alapuranen (LAUREA),	Outlines of D8.11
0.2	31/08/2021	Juhamatti Etuaro	First version of D8.11
0.3	16/09/2021	Juhamatti Etuaro	Modified after comments
0.33	1/10/2021	Juhamatti Etuaro	Modified 3.1, 3.2 and 4.1 after language checking
0.34	19/10/21	Juhamatti Etuaro	Modified after internal review
1.0	31/10/21	Juhamatti Etuaro	Last amendments

Table of Contributors

Table 2 Deliverable Contributors

Section	Author(s)
1 Introduction	Nina Alapuranen (LAUREA), Juhamatti Etuaro (LAUREA), Sari Sarlio-Siintola (LAUREA), Rauno Pirinen (LAUREA)
5.1 DPIA in SHAPES project	Nina Alapuranen (LAUREA), Juhamatti Etuaro (LAUREA)
1-5	Juhamatti Etuaro (LAUREA), Commented by: Sari Sarlio-Siintola (LAUREA), Rauno Pirinen (LAUREA), Nicola Goodfellow (NHSCT), Michael Scott (NHSCT), Artur Krukowski (ICOM)

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

Table of Acronyms and Abbreviations

Table 3 Acronyms and Abbreviations

Acronym	Full Term
DG	Directorate-General
DGA	Data Governance Act
DPA	Data Processing Agreement
DPO	Data Protection Officer
DPIA	Data Protection Impact Assessment
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EHDS	European Health Data Space
ENISA	The European Union Agency for Cybersecurity
FAIR	Findable, Accessible, Interoperable and Re-usable
GDPR	General Data Protection Regulation
NIS	Network and Information Systems
PT	Pilot Theme
SCC	Standard Contractual Clauses
TEHDAS	Towards the European Health Data Space
UC	Use Case
WP	Work Package
WP29	Article 29 Data Protection Working Party (EDPB's predecessor)

Keywords

Privacy, Data Protection, GDPR, Data Strategy, European Health Data Space, DPIA, Secondary use, Legal basis, Anonymisation

Disclaimer

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 Tables

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

Executive Summary

This first version of deliverable Privacy and Data Protection Legislation in SHAPES (D8.11) in M24 will focus mainly on the SHAPES piloting phase, while D8.12 shall orientate focus on the time after the SHAPES project concludes. The main purpose of this document is to assess how the current privacy and data protection legislation have been complied with, and also to give tools to the SHAPES partners for achieving and demonstrating this compliance.

The most important legal act concerning data protection within the internal market is Regulation (EU) 2016/679 (GDPR), which has nonetheless left the situation of data re-use rather vaguely regulated. Therefore, the Commission has announced a European strategy for data that will introduce different sectoral data spaces, including the European Health Data Space (EHDS, e.g., Digital Health Europe – Consultation with Industry on the European Health Data Space, https://digitalhealtheurope.eu/wp-content/uploads/2020/10/EHDS-Industry-Report.pdf).

The legal basis for the processing of personal data in the SHAPES project is consent (Article 6(1)(a) and Article 9(2)(a) GDPR). The main reason for this is that in a pan-European project, it is a solution that fits all of the Use Cases. It can be seen appropriate when data is collected directly from data subjects. The consents will be requested in a written template, and alongside it, the data subject will be provided with an information sheet in accordance with Articles 12 and 13 GDPR.

As is required in Article 28(3) GDPR, all the processing operations in SHAPES will be governed by a contract. For situations where a partner resides in the UK's jurisdiction, there is a slightly amended version in place, which also contains referrals to the UK Data Protection Act 2018 in relevant parts. The idea is that the data protection level provided in the GDPR is not decreased, but it merely takes the national rules into account for parties in the UK; thereby, in this case, providing additional protection, because the GDPR as itself is no longer applied in the UK.

Legislation concerning the secondary use of health-related data is fragmented within the EU. Generally, if further research is not specified accurately enough, such processing may be classified as 'further processing', and as such may be prohibited; because data may not generally be subjected to further processing in a manner that is incompatible with the purpose stated at the time of collection (Articles 5(1)(b) and 6(4) GDPR). Anonymisation could be an answer to these issues, but Member States' authorities interpret it differently. Some of them believe that health-related data cannot remain useful while anonymised, and this makes open sharing difficult at this point. Upcoming supranational legislation is seen in the literature as the only workable answer.

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

SHAPES' partners will conduct data protection impact assessments before starting any personal data processing. The data protection manager will support this work. For fulfilling the GDPR requirements, data security and risk related workshops have been held.

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

1 Introduction

It has been considered that this first deliverable on Privacy and Data Protection Legislation in SHAPES (D8.11) serves its purpose best by focusing mainly on the piloting phase of the SHAPES project. In the second version, D8.12, the questions that have arisen in the pilots and during the project, the ecosystem and business modelling will be discussed, having the focus on time after the SHAPES project has concluded.

SHAPES will collect a significant amount of personal data. The data will mainly be collected as part of the pilots conducted during the SHAPES Innovation Action. While collecting data, SHAPES' partners need to ensure that all relevant privacy and data protection legislation will be taken into account before the data processing starts. To help pilots in implementing privacy by design and privacy by default principles, WP8 has already provided a list of privacy and data protection requirements as part of the SHAPES Ethical Framework (D8.14, see also Ethical and Legal Requirements in Final User Requirements D3.9). Work Packages that process personal data during the project have been able to take these requirements as part of their planning. D8.14 also gave concrete instructions on how the different GDPR requirements should be implemented.

SHAPES collects personal data from various different sources and processes it in different ways. Data will be collected by mechanisms including sensors, applications, interviews and questionnaires. Also, in certain Use Cases, non-IoT medical data will be processed. To ensure that individuals' rights will be respected and the processing will be compliant with privacy and data protection legislation, SHAPES will conduct Privacy and Data Protection Impact Assessments (DPIA) for the pilots and in some cases also for the pilot use cases. This task developed templates for conducting DPIAs and the process for conducting those.

While it is important to ensure that individuals are protected, SHAPES has also a goal to ensure that the FAIR data principles can be also followed in all cases where the data originally collected includes personal data. The EU has a strong vision for data sharing in the health and care sector in Europe, and SHAPES needs to consider if the collected data can be used for other purposes. There is a clear need and value for sharing the data for secondary use, but the challenge is that the legal ground for this is not clear at the moment. This deliverable will describe the challenges but also introduce the steps that SHAPES will take to bring more clarity to the topic.

Another issue that has caused a lot of discussion around the organisation is personal data processing outside the EU/EEA. As a guiding principle, it has been decided that all SHAPES data needs to be processed inside the EU/EEA. This is not without exceptions, though, as some of the SHAPES partners reside within the UK. Nonetheless, this seems to have only a slight impact on the project, since the

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

Commission only recently presented an implementing decision on the adequate protection of personal data by the UK (C(2021) 4800 final). Having the data mainly processed within the EU/EEA is difficult, since SHAPES needs to use cloud services for building up the ecosystem and running the pilots. In those cases, there is a risk that the data will be transferred outside the EU. In this deliverable, it is explained how SHAPES has ensured compliance with GDPR and that authorities' opinions have been taken into consideration when both the decisions of the technologies used and data storages have been decided.

1.1 Rationale and purpose of the deliverable

The main purpose of this deliverable is to give SHAPES' partners tools they can use to ensure and demonstrate that the data processing during the pilots is compliant with privacy and data protection legislation, mainly with GDPR. As most of these matters have already been discussed within meetings and in D8.14, this document can be relied on as a support mechanism when different pilot sites commence with their, e.g., DPIA processes. Conducting DPIAs is a huge effort for the pilots, and the aim for this deliverable is also to help partners execute the DPIAs by using the work that has already been done in other work packages, like D8.13 data management.

This deliverable will also provide background for discussion on the secondary use of SHAPES data. As the regulatory situation within the EU is fragmented, the question on this matter is complicated. Hence, in order to provide a clear image of the possibilities for the re-use, grounds for the current interpretations concerning the topic must be explained. Anonymisation remains a big part of the discussion, and the legal aspects of it need to be explained in a detailed manner. Also, because the regulatory situation is under pressure to change, it is relevant from the SHAPES project's point-of-view to cast a light on the regulatory initiatives that are being planned and that have already taken place. For these goals to materialise, observations will be made based on the following:

- Current EU legislation in force
- Official EU documents, such as proposals for regulations, impact assessments and, e.g., recommendations from EU authorities
- Legal literature
- Outcomes and published articles of other relevant projects

1.2 Deliverable Objectives

- Prepare templates and instructions for conducting SHAPES DPIAs in pilots
- Provide instructions and template for conducting Data Processing Agreements within SHAPES pilots
- Update SHAPES privacy and data protection policy after DPIAs as required
- Instruct on how the data security arrangements are to be described

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

- Highlight the possibilities regarding the secondary use of data for, e.g., scientific research
- Address the transfers into third countries or international organisations
- Describe the reasoning behind the chosen legal basis in the Use Cases

1.3 Structure of the document

Firstly the subject matter of this document is outlined in the introduction. The rationale and purpose of D8.11 are explained in section 1.2, and the objectives are detailed in section 1.3. They will help the reader get an overview of the matters that will be assessed as a minimum.

After describing the objectives, the focus moves to applicable EU legislation. Besides listing and explaining the currently applicable legal rules, upcoming relevant directives and regulations will also be specified. Some of the relevant proposals, such as the one for European Health Data Space, have not been published yet; but because of their importance for the project, they will be discussed in more detail in later sections.

Section 3 concerns the legal basis for the processing of personal data. First, the general reasoning for the following question is presented: why is the legal basis chosen to be consent, instead of for example, public interest? As this aspect affects the project's opportunities for secondary use and obliges the data controllers to certain procedures, it will be thoroughly explained. Also, the matters of data processing agreements and collecting personal data are covered in section 3.

In section 4, the big questions regarding secondary use of personal data will be addressed. As the sharing of data is widely hoped for, the current situation of the secondary use of health-related data is summarised alongside anonymisation, which is closely related to the matter. In the final sub-section, 4.3, the possible solutions for the difficult regulatory situation will be assessed. They include new legislation that is in preparation and also upcoming guidelines from the European Data Protection Board.

The final section, 5, is dedicated to matters relating to the data protection impact assessment (DPIA). In this section, the general obligations to conduct a DPIA and the SHAPES project's approach to it are explained. In the sub-sections, the procedures for certain parts of the DPIA process are described, i.e., the project's risk assessment workshops and how the data security measures are to be presented. Finally, the question of transferring data into third countries will be briefly addressed.

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

2 Applicable Union legislation

The most relevant legal act is Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Although it covers the vast majority of situations involving data processing, it leaves questions about the secondary use of data, mostly to be answered by the Member State legislators and authorities, providing only a summary framework for them. Hence, secondary use causes legal uncertainty and, as expected, Member State authorities have taken different approaches to the matter, leaving the field of legislation fragmented.

The situation has not gone unnoticed by the EU, and the European Commission has left a proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act, DGA), dated 25.11.2020, in order to facilitate data sharing across the EU and between sectors. The DGA introduces conditions under which public sector bodies may allow the re-use of certain data they hold, notably data which is protected on the grounds of commercial confidentiality, statistical confidentiality, protection of intellectual property rights of third parties or the protection of personal data. Additionally, it imposes obligations on providers facilitating the sharing of personal and non-personal data. It also addresses the questions of data altruism, making it easier for natural persons to allow the secondary use of their personal data.

Nevertheless, as will be seen in Chapter 4.2, it is argued by many stakeholders that mere horisontal regulations, such as the upcoming DGA, cannot address the specificities of health-related data; therefore, the Commission has announced its plans for the European strategy for data, with which different sectoral data spaces will be put into place. Also, the European Health Data Space will be part of this, and the European Council has stated that this particular area should be made a priority.

Other relevant legal acts are, e.g., Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive), Directive (EU) 2015/1535 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) and Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive).

A proposal for e-Privacy Regulation (COM/2017/010 final - 2017/03 (COD)) has been adopted, which would replace the e-Privacy Directive, but also for a revised Directive on Security of Network and Information Systems (NIS 2 Directive).

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

3 Legal basis for the processing of Personal Data

3.1 Reasoning for the legal basis in the SHAPES project

As it is stated in Article 6(1)(a) GDPR, the processing shall take place only after the data subject has given consent to the processing of his or her personal data for one or more specific purposes. Although there are other legal bases for conducting research, consent can be seen as most appropriate for the context of SHAPES pilots, as the data is being collected directly from the data subject. Consent can also be obtained with a relatively little effort in each Use Case. That would not be so in large-scale research projects with vast numbers of participants involved. Also, by utilising consent, it is rather simple for the data subject to make decisions on using his/her personal data in the project at any point. By withdrawing their consent all of the processing activities on their personal data that the consent applies to must be stopped and respectively all of the identifiable personal data must be erased.

Another reason for using consent as a legal basis is that an explicit consent allows processing of special categories of personal data (Article 9 GDPR). According to the Article, processing of personal data concerning the data subject's health shall be prohibited, but that does not apply if one of the exceptions listed in the Article's paragraph 2 applies. Article 9(2)(a) provides that if the data subject has given his/her explicit consent the prohibition referred to in paragraph 1 shall not apply.

It could be problematic to use public interest as a legal basis in all parts of the SHAPES project, because according to DG Health and Food Safety's Assessment, variation exists between Member States in how they distinguish between public and non-public sector researchers. The definition affects the selection of legal basis and it could be difficult for researchers in for-profit organisations to prove that research is in the public interest. As stated in D4.1 (SHAPES TP Requirements and Architecture, p. 46), there is a commercial version of SHAPES to be expected. In this sense, it seems apparent that the project is not at least thoroughly conducted in the public interest, and thereby, the consent seems to be viable option for the project, as it can result in marketable solutions.

Consent is obtained using a common consent template and an information sheet, which is provided for the participant before signing the consent form. Both templates have been written alongside the deliverable SHAPES Baseline for Project Ethics (D8.2). As the personal data required for the processing can vary from Use Case to Use Case, the Pilots have been instructed to write the templates in accordance with the purposes for which the data will be processed. The information that all of the templates must contain consists of the general information of the study in question, such as the voluntary nature of participation, possible advantages or disadvantages, and the annex that contains the privacy policy.

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

Along with the consent form, the data subject is provided with a Use-Case-specific information sheet, where the existence of the data subject's rights (Chapter III GDPR) has been described and how to use them. On the information sheet, basic information is also listed, such as the controller's identity, purpose of each of the processing operations for which consent is sought, what data will be collected and the existence of the right to withdraw consent (EDPB Guidelines 05/2020 on consent under Regulation 2016/679, p. 15: the minimum content requirements for consent to be informed). As stipulated in Article 7 GDPR, it shall be as easy to withdraw as to give consent.

If relevant, the sheet will also contain information about automatic decision making and possible risk of data transfers due to the absence of an adequacy decision of appropriate safeguards, as described in Article 46 GDPR. It can be clarified here that most likely none of the Use Cases contain any actual automatic decision making, because there is always a human assessing the results of any profiling; therefore, a human always gets to make the final decision.

The elements of a valid consent are provided in Article 4(11) GDPR. According to it, consent by the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. As stated in Recital 43, consent cannot be considered freely given if there is a clear imbalance between the data subject and the controller. It is, therefore, important that a data subject is not pressured and does not suffer from disadvantages if they decide not to give consent.

The requirement for the consent to be informed means, in the context of SHAPES, that the data controller needs to accurately describe, for instance, how the data subject's rights are safeguarded, what happens to the personal data during the research and how they are dealt with when the research activities have ended. According to the guidelines 05/2020 of the EDPB (p. 14), the requirement that consent must be specific aims to ensure a degree of user control and transparency for the data subject. This requirement has not been changed by the GDPR and remains closely linked to the requirement of 'informed' consent. Still, the consent may cover different operations, as long as these operations serve the same purpose. Lastly, when it comes to the indication of the data subject's wish for consenting being unambiguous, the request will not be presented amidst a large bulk of text, but as a separate form, which clearly explains the procedure in question. As stated in D8.14, consent shall be requested in a manner clearly distinguishable from other matters and in an intelligible and easily accessible form, using clear and plain language.

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

3.2 Data Processing Agreements

According to Article 28(3) GDPR, any processing by a processor shall be governed by a contract or other legal act under Union or Member State law, which is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. In order to ensure compliance with the requirements of paragraph 3's subparagraphs (a)-(h), it has been decided to utilise the Commission's standard contractual clauses (Commission Implementing Decision (EU) 2021/915) in the SHAPES project.

In some of the situations, where the controller and/or the processor reside in United Kingdom, the standard contractual clauses have been supplemented with referrals to relevant sections of the UK Data Protection Act 2018 to ensure compliance with also the national legislation. This has been done as a precaution even when it might not be necessary, as the GDPR sets the stricter requirements for data protection. The EDPB has stated in its guidelines 07/2020 that it will be possible for the parties to add additional clauses (e.g. applicable law and jurisdiction) as long as they do not contradict, directly or indirectly, the SCCs and they do not undermine protection afforded by the GDPR and EU or Member State data protection laws.

The supplementary clauses in question have been formed as such that they do not contradict with the SCCs. For example, the Clause 3(c) requires that "These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725 and/or, when relevant, United Kingdom's Data Protection Act 2018 (c. 12) or in a way that prejudices the fundamental rights or freedoms of the data subjects." They can even theoretically raise the level the protection, because, according to the wording, if the UK law in some occasions demands higher protection or prohibits some activities, the parties also need to abide by those prohibitions. There is no situation where the supplementary clauses allow any processing which would be forbidden in the GDPR.

Although according to the EDPB's guidelines 07/2020, the concepts of controller and processor are functional in that they aim to allocate responsibilities according to the actual roles of the parties; thereby, the roles stem directly from the factual activities and relationships between the parties, the SHAPES partners have been instructed to identify those roles and fill the Data Processing Agreements (DPA) accordingly. That means the DPAs do not designate the roles by themselves, but obviously it is crucial to have the roles and their respective responsibilities planned before any actual data processing activities take place. Insofar as some other entity was actually deciding the purposes and means of the processing and hence deemed as a controller, it would also immediately assume the responsibilities of the controller in the eyes of the law, and the consequences could be detrimental for different parties. In a case where a

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

data protection authority, national or supranational, considered that the obligations set in the GDPR have not been abided by, it has a right decreed in Article 58(2)(f) to impose a temporary or definitive limitation, including a ban on processing, and ultimately, an administrative fine could come into question.

As identifying the roles is sometimes simple, but in other cases rather complicated, some of the SHAPES Pilot Sites have found the assistive chart created by the EDPB (published in the guidelines 07/2020) helpful. Because it has become relevant in the context of SHAPES, it is included in this deliverable as well as in Annex I. The EDPB has instructed in the identifying process, that deciding on essential means, such as what type of data and how long it will be processed, is inherently reserved to the controller. Also, the processor can make certain decisions on non-essential means, which could be used as hard- or software or the technical data security measures. As defining the means answer to the question “how”, the purposes of the processing answer to the question “why”. It is not sufficient to merely state, e.g., “to advance the project”, since according to Article 5(1)(b) (purpose limitation) personal data shall be collected for specified purposes and not further processed in a manner that is incompatible with them. Therefore, a certain degree of accuracy in describing is required. It must be clear to the reader as to what end this particular processing operation is taking place.

The main rule is that the operator of the SHAPES Pilot Site assumes the responsibilities of the controller and the Digital Solutions providers are the processors as they, for instance, analyse the data provided for them. Identifying the roles occurs in most cases while carrying out the Data Protection Impact Assessment, in which the SHAPES Data Protection Manager provides support. It is also assessed within the DPIA processes if some of the partners factually determine jointly the purposes and means of processing and thereby become joint controllers, as it is described in Article 26 GDPR.

The template for the Data Processing Agreement can be found in Annex II. It has to be clarified that the version included in this deliverable is the one intended for the cases where some of the partners reside in the UK. The supplementary clauses have been highlighted with light blue. Although it has been written in a way that those clauses should not matter in cases where no UK legislation is involved, this version is only meant for the controller-processor relationships, where some of the parties do reside in the UK. Therefore, in most cases, just the standard contractual clauses are applied.

While this deliverable is being written, there is also in preparation a separate agreement template for sharing personal data acquired by harmonisation questionnaires between the pilot sites and Maynooth university. This data is used mainly for analysing the outcomes of the whole project, but also for analysis performed by the pilot sites for writing scientific articles based on it. These activities will happen as part of SHAPES project and the data subject will be informed on them. It has been

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

seen appropriate to have a sharing agreement in place for controller to controller situations in order to demonstrate compliance with GDPR, as it is stated in Articles 5(2) and 24(1).

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

4 Secondary use of personal data

4.1 General remarks regarding the secondary use

The concepts of primary and secondary use of personal are widely used in reports and literature, but not defined exhaustively in the GDPR. Instead, Recital 50 GDPR speaks of the processing of personal data for purposes for which the personal data were initially collected and, respectively, of other purposes than those for which the personal data were initially collected. When it comes to patient data, the processing for the purposes of provision of health and social care by health and care providers to the patient concerned is generally referred to as a primary use. The secondary use comes into play when the data is processed for some other purpose.

On the other hand, if the data is collected primarily for scientific research purposes, then the processing for these purposes will constitute the primary use. It is important to note, that any potential further activities that may be undertaken beyond the primary processing should also be specified to the data subject. If not specified accurately enough, such processing may be classified as 'further processing' of data, and as such may be prohibited under the GDPR, because data may not generally be subjected to further processing in a manner that is incompatible with the purpose stated at the time of collection (Articles 5(1)(b) and 6(4) GDPR). For instance, open sharing of data initially collected for scientific research would unequivocally be secondary use.

Article 14(4) GDPR provides, that where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2. It is recommended for the pilot sites to plan the needs for processing of personal data as far as it is possible and request consents for them accordingly, so the secondary use or the need for re-consenting would not have to be considered. In patient data's case, it has to be noted, that it falls within the scope of special categories of personal data meant in Article 9 GDPR. Further processing of special categories is usually regulated in Member States legislation far more strictly than further processing of "normal" personal data.

Although it is stated in Recital 33 GDPR that "It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose"; according to the EDPB guidelines 05/2020 (p. 30), it should be noted that Recital 33 does not disapply the obligations with regard to the requirement of specific consent. This means that the Recital 33 cannot be relied on when it comes

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

to the secondary use of personal data. Knowing that defining the purposes of research activities may be sometimes difficult, this cannot be taken advantage of, e.g., by writing the purposes intentionally in a vague manner. Moreover, the EDPB states that a lack of purpose specification may be offset by information on the development of the purpose being provided regularly by controllers as the research project progresses so that, over time, the consent will be as specific as possible. This makes it possible for the data subject to assess more accurately his/her willingness of participating and using the right to withdraw the consent.

Article 9(4) GDPR stipulates that Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. In the DG Health and Food Safety's Assessment of the EU Member States' rules on health data, in the light of the GDPR (p. 58), it is stated that the Member States have not implemented further legislation on the secondary use in a homogenous way, which has resulted in a fragmented field of legislation, hampering the researchers' work.

Also, according to reports (TEHDAS: Why health is a special case for data governance, 2021, p. 22), only a few EU Member States have nationwide and centralised regulatory frameworks for the access and re-use of health data in national law. Furthermore, these collaborations and (cross-border) exchanges of data may be governed by subnational regulations or even lower governance structures. This causes fragmentation and hampers the unambiguous access and exchange of health data, which in turn proves the need for a more unified regulatory framework.

Because the matter is regulated differently in different Member States (as well as in the UK), the data controllers in the SHAPES project are advised to investigate the national legal rules relevant for them in order to access and use any patient data for research. In some Member States, certain stakeholders can block the release of patients' data for research even if the patient has consented, if, for instance, the Research Ethics Authority refuses to grant permission.

4.2 Anonymisation as a key to re-use?

In the DG Health and Food Safety's Assessment of the EU Member States' rules on health data, in the light of GDPR, it was noted (p. 61) that, in practice, some Member State authorities work on the basis that full anonymity can never be achieved for health-related data while still keeping the data useful for research; others believe anonymity within the meaning of GDPR can be achieved. For instance, according to Groos & van Veen (2020, 2), the opinion 5/2014 of the WP29 on anonymisation techniques and the Dutch Data Protection Authority subsequently, state that because of new techniques, which the holder of the data cannot influence, one can never be sure whether anonymous data might become personal data again. As the EDPB still

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

promotes its interpretation stated in the opinion 5/2014, they see that the anonymous route to secondary use has de facto been made illusory.

This makes it difficult for a pan-European project, such as SHAPES, to organise open data sharing as a form of secondary use, as the views of the national authorities can differ radically from each other. In the case of open sharing, it should be aligned to the strictest standards of all the Member States in order to be sure, and in that situation, the results would probably not be of value for neither the sharing nor the re-using party. As stated in the DG Health and Food Safety's Assessment, anonymous data, to the highest standards without any residual risk for re-identification, may lose their value for nuanced research. Also, Groos & van Veen (p. 7, 2020) think there is always a trade-off between the usability of the data for research and the level of anonymisation.

Furthermore, anonymisation as such is still an act of data processing and must be legitimised under GDPR. According to the DG Health & Food Safety's Assessment (p. 137), clarifications are however needed under which conditions the further processing of data in order to render them anonymous for the purpose of scientific research would be legitimate, and when data can really be considered anonymous. It is still recommended for the pilot sites to request a consent for this purpose as well.

In the larger picture, the processing of biometric data for the purposes of identification has also been seen in literature (Korja 2016, 164) as a factor reducing the effect of anonymisation. In certain Use Cases of the SHAPES project, a solution for facial recognition will be implemented (D6.1, 46). Additionally, there are plans to utilise virtual voice assistant services.

According to GDPR 5(1)(b), further processing for scientific research purposes (in public interest) in accordance with Article 89(1) is not considered incompatible with the principal purpose. It is difficult to see SHAPES as a project conducted thoroughly for public interests, since there are commercial interests mixed in. As it was described earlier in Section 3 (Legal basis), the public and the commercial interests do not always coincide. Even if the processing based on public interest could be justified, another matter is, how can it be guaranteed that the further processing after making the data available would be for scientific research purposes in the public interest? This question relies on the interpretation of some of the Member States' authorities that the data cannot be fully anonymised while still keeping it useful for research. Thereby, if the data can be even theoretically considered identifiable, it is essential to know and specify the further purposes. In this context, the EDPS has stated that where trust plays such a crucial role, performing an activity deemed to be research cannot be a carte blanche to take irresponsible risks.

Mourby (2018) strongly supports the relative approach to anonymisation. In other words, in her view, a level of anonymisation that keeps the data viable for secondary use can be achieved. According to her article (p. 229, 2018), the GDPR increases the scope of personal data to the detriment of research. Still, although in Recital 26 GDPR,

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

it is stated that the Regulation does not concern the processing of anonymous information, even she does not propose that the anonymised data would be openly shared; instead, there would be control mechanisms for assessing the entities that are requesting access to the data, trustworthiness. Also, Groos & van Veen (p. 2, 2020) say in their article that not everything goes once data has been anonymised. Thereby, even among the researchers who disagree with the absolute approach, it is seen that some control must be retained over the anonymised personal data.

Due to the views presented above, the possibilities for any secondary use of personal data – especially when speaking of the special categories – must be approached cautiously. As the topic is being discussed widely at the EU level and national level, too, in the next chapter, the legislators' reaction to the presented regulatory issues will be observed. As the situation may seem complicated, the European Data Protection Board has announced that the development of a further and more detailed guidance for the processing of health data for the purpose of scientific research is part of the annual work plan of the EDPB in their guidelines 03/2020.

4.3 Upcoming supranational legislation: the European strategy for data and the European Health Data Space

The European Commission has outlined a European strategy for data in the communication COM/2020/66 final. The strategy ultimately aims to strengthen the European Single market by addressing several questions regarding the free flow of data that has been seen as problematic. According to the Commission, common European rules and efficient enforcement mechanisms should ensure the following:

- data can flow within the EU and across sectors
- European rules and values, in particular personal data protection, consumer protection legislation and competition law, are fully respected
- the rules for access to and use of data are fair, practical and clear, and there are clear and trustworthy data governance mechanisms in place
- there is an open, but assertive, approach to international data flows based on European values.

In the special meeting of the European Council of 1 and 2 October 2020 (EUCO 13/20), the European Council "welcomes the European strategy for data, which supports the EU's global digital ambitions to build a truly European competitive data economy, while ensuring European values and a high level of data security, data protection, and privacy. It stresses the need to make high-quality data more readily available and to promote and enable better sharing and pooling of data, as well as interoperability. The European Council welcomes the creation of common European data spaces in strategic sectors, and in particular invites the Commission to give priority to the health data space, which should be set up by the end of 2021."

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

In the combined evaluation roadmap/inception impact assessment (Ares(2020)7907993, p. 2) of the European Health Data Space (EHDS), it has been recognised that access to, and exchange of, health data for scientific research and innovation, policy-making and regulatory activities remain very limited in Europe. This is mostly because the GDPR is being interpreted differently in different Member States. According to the assessment, the baseline scenario does not promise: "sectoral aspects, such as the types of data and modalities for access would not be addressed, leaving the access to and re-use of health data to a large part still fragmented, limiting the effectiveness of public health action such as in the case of infectious diseases (e.g., COVID-19) or rare diseases." Therefore, the sort of measures that should be adopted in order to answer these, so to say, regulatory deficiencies has been assessed.

The Directorate-General for Communications Networks, Content and Technology wound up identifying (SMART 2019/0024) the so-called low-intensity regulatory intervention as the preferred policy option. It encapsulates requiring Member States to set up a one-stop shop that would facilitate data discovery for re-users while providing technical and legal advice to holders, along with secure data processing environments ensuring the security of the data. These services would only be available to entities established in the EU, and on a level-playing-field basis.

As mentioned earlier, the Commission has adopted a proposal for the Data Governance Act. Still, it is widely thought that such a horisontal proposal, which lays down a governance framework for the common European data spaces, can address these limitations only partially due to the specificity of health data. This question has been assessed within the framework of the TEHDAS (Towards the European Health Data Space) project, which is described as a joint action that helps EU member states and the European Commission develop and promote concepts for the secondary use of health data to benefit public health and health research and innovation in Europe.

Like the SHAPES project, TEHDAS also divides into different work packages. Its WP4 is about outreach, engagement and sustainability, and within the context of that work package a project forum, which aims to identify the relevant initiatives and projects across the EU, is arranged. Through this forum, the different projects and initiatives will also connect to other relevant WPs within TEHDAS where collaboration and synergies are possible. Also, the SHAPES project has participated in this forum.

The TEHDAS project has identified a list of barriers to data sharing, of which most are legal (https://tehdas.eu/news/tehdas-identifies-barriers-to-data-sharing/). It could be said that the common denominator between them is the fact that the

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

Member States can make different interpretations of the GDPR in their national legislations. Much is to be expected from the TEHDAS project, as within its WP6, for instance, guidance on ensuring data quality, such as the anonymisation of data, is being developed.

The initiative of European Health Data Space will result in a proposal for a regulation, although the contents of it have not been published yet. The initiative has been in its public consultation phase, and the feedback period ended on 26 July 2021. Many members of the public have participated, outlining the biggest issues in the current regulatory situation and things to be avoided when writing the legal text. In the work programme for 2021, the Commission has planned the EHDS legislative proposal for Q4/2021.

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

5 Privacy and Data Protection Impact Assessment (DPIA)

5.1 DPIA in the SHAPES project

The GDPR article 24(1) requires that controllers implement appropriate technical and organisational measures to ensure and be able to demonstrate compliance with the GDPR. Article 24(2) also states that where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller. One way to demonstrate the compliance and identify potential risks is to conduct a DPIA that is described in article 35 of the GDPR. Article 35(1) refers to a likely high risk "to the rights and freedoms of individuals". Although DPIA is required only in cases where a type of processing is likely to result in high risks to the rights and freedoms of a natural person, the EDPB highlights that the controllers' general obligation to implement measures to appropriately manage risks for the rights and freedoms of the data subject still remains, although the criteria for "high risks" would not be met. (Article 29 Data Protection Working Party 17/EN WP 248 rev.01, page 6.).

According to the GDPR article 35(3), a DPIA is also required in a case where processing consists on a large scale of special categories of data. SHAPES will have several different types of pilots, where in some cases, the data collected will contain special categories of data, and in some cases, the amount of data collected is large. It has to be noted that some of the Use Cases involve the processing of biometric data for the purposes of identification. The biometric data includes facial recognition, and also processing of voice data in the form of virtual voice assistant services, which by their nature are mostly provided by major corporations.

Additionally, in some of the Use Cases, there can be some unintentional collection of personal data, such as location data when the data subject is providing video material to the controller or processor. In such situations, it is necessary to have a plan to act in accordance with the principle of data minimisation, and therefore, to erase all unintentionally collected personal data. Data minimisation should be addressed when it comes to virtual voice assistants, too, since they could accidentally collect information from people unrelated to the SHAPES project.

Due to the variety of the pilots, and taking into account that the pilots are aimed at elderly individuals, it has been decided in the Grant Agreement that all SHAPES pilots shall conduct a DPIA, even if it would not be necessarily required by the GDPR. This is also part of SHAPES' ethical goals to identify potential risks and mitigate those in a way that the processing will be safe for the individuals.

The SHAPES DPIA consists of three parts: Data processing descriptions, written DPIA document and risk analysis. Templates have been structured in a way that pilots can

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

utilise work already done for other areas so that duplication can be avoided. For instance, content for the data processing descriptions can be taken from data plans that pilots will do when planning the pilot and data collection. Risk analysis work will be utilised in SHAPES' privacy and Risk management deliverable, and DPIAs will then eventually be used for modifying the SHAPES privacy and data protection policies if needed.

All pilots will do a DPIA before the personal data processing activities in the pilot starts. Because SHAPES has different types of pilots, it has been agreed that the pilot lead together with the pilot site DPO will decide if it's better to do one DPIA for the whole pilot or do singular DPIAs for each use case. The risks will also be identified from all locations' points of view to ensure that local legislation will be covered as well. DPIAs, and especially the related risk analysis, will be done in co-operation with the parties who take part in the pilot planning and execution. It requires expertise on several areas so that it can be ensured that all different risks for individuals have been taken into consideration. This applies especially for the risk management part.

The SHAPES Data Protection Manager supports pilots in their DPIA work. WP8 has provided templates, arranged trainings for the pilot DPOs and pilot leads and created instructions on how to fill in the DPIA templates, and what aspects should be taken into consideration when the DPIA is under preparation. The SHAPES Data Protection Manager shall keep a consolidated list for processing activities in SHAPES and will also analyse all the DPIAs to ensure that those are consistent and to assess if there are some risks that are identified in multiple DPIAs and that would require a more detailed analysis.

The main goal for the DPIAs is to ensure that all privacy and data protection requirements set in D8.14 have been implemented and that there are no such risks that could prevent the pilot from going live. The assumption is that while pilots are following the privacy by design approach, there will be no major risk findings, but this will work as a final check. It will also fill the SHAPES accountability obligation. SHAPES has also decided to slightly widen the DPIA scope from traditional DPIAs. Because FAIR data principles that are introduced in D8.13 Data Management Plan play an important role in the SHAPES ecosystem, pilots will also decide what part of the collected data can be shared within SHAPES and with third parties.

The usage of data for secondary purposes is presented in section 4 of this document. The reason for taking this topic as part of the DPIA is to ensure that data processing activities have been planned in a way that it allows both the protection of the personal data and the data-sharing activities in a way that there will be no risks for the individuals taking part in the pilot.

In the actual DPIA document, the pilot sites are asked to describe their data flows, i.e., how and from where they will receive the data, where and how long the data will be stored and whether the data will be transferred to third parties. The data flows are

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

recommended to be described first in words and after that with a data flow diagram. The SHAPES partners have been prompted to make their data mappings so that describing the data flows in the form of a data flow diagram would be a convenient place to start filling in the template. It would also support the whole pilot site's DPIA process, as it could make them aware of the roles that different partners have in their particular Use Case. Identifying the roles is of utmost importance, since, as described in Chapter 3.1 (Data processing agreements), the GDPR requires that any processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller. Hence, the data processing agreements need to be in place before the data processing can start. Also, as known, the roles must be assigned and described in the descriptions template.

The GDPR does not impose an obligation on the controller of publishing the DPIAs made for their processing operations. Still, according to the WP29's guidelines on DPIA and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev.01, subsequently endorsed by the EDPB, 1/2018), although publishing a DPIA is not a legal requirement of the GDPR, it is the controller's decision to do so (p. 18). The WP29's/EDPB's view is that the purpose of such a process would be to help foster trust in the controller's processing operations and demonstrate accountability and transparency.

It is, however, encouraged by the WP29 to consider publishing at least parts, such as a summary or a conclusion of their DPIA. Therefore, and taking into account that one of the objectives in the SHAPES project is producing information that could be made available for the public, it should be considered if such summaries or conclusions could be published. The DPIAs in their wholeness probably cannot be published, because, as the WP29 has stated: the DPIA could present specific information concerning security risks for the data controller or give away trade secrets or commercially sensitive information.

5.2 Procedures for identifying and addressing risks

As mentioned in section 4, Article 35(1) refers to a likely high risk "to the rights and freedoms of individuals". In order to comply with the legal requirements, a process for identifying, assessing, and mitigating the risks in question will be performed alongside every DPIA in a uniform manner. The risk assessments may also contain risks not directly related to data subjects' rights and freedoms, but instead data management-related risks and risks for research activities. This is not the main focus, but as they may indirectly affect the data subjects as well, the comprehensive approach has been encouraged. A short description of the process chosen for these tasks is provided here, but a more substantive coverage of the SHAPES risk assessment can be found in the Deliverable 8.9 (First SHAPES Privacy and Ethical Risk Assessment).

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

Many of the identified risks apply to many of the Use Cases because there are plenty of Digital Solutions that provide their products or services in a similar manner to different data controllers. Therefore, it has been considered best for the project to arrange special workshops for identifying, assessing and addressing the risks. This way, duplicate work can be minimised, which, on the other hand, could result in inconsistencies. For instance, the assessed severity of risks could mismatch between Use Cases, and in some situations, a relevant risk could be left out. In some cases, this could be justified, but having risks assessed in a wider context than within a single Use Case can be seen as enhancing the quality of risk assessments.

The identified risks of a collective nature will be collated into a single document, which can be used as a support in the DPIA processes thereafter. After the risks have been collected, the relevant partners gather again in a second larger risk meeting, where opinions can be shared and the findings further discussed.

5.3 Describing the data security measures

As it is stated in Article 35(7)(d) GDPR, the assessment shall contain, inter alia, the description of the implemented security measures. The measures are generally divided into technical and organisational measures. The general obligation for implementing data security measures is stipulated in Article 32, titled “security of processing”. The list (a)-(d) provided in the Article is not exhaustive, as can be interpreted from the expression “inter alia as appropriate”. On the other hand, all of the measures listed there do not necessarily have to be implemented, but only those which are appropriate in the processing operation in question. Therefore, the measures may include, e.g., pseudonymisation and encryption, the ability to ensure the ongoing confidentiality and integrity, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and a process for regularly testing the effectiveness of the implemented measures.

The GDPR has adopted a technologically neutral approach to data security measures. It thereby avoids naming any specific solutions, and instead focuses on describing the desired results. One of the benefits characteristic to this approach is that the obligation to actually implement adequate measures is harder to circumvent. In Recital 15 GDPR, it is stated that the GDPR: in order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. Still, according to Mondschein & Monda (p. 58, 2019), this approach could introduce a sense of legal uncertainty, because it requires a lot of expertise to decide on the means.

Another set of requirements (or suggestions) can be found in the Deliverable 8.14’s (Final SHAPES Ethical Framework) section 6 (Cybersecurity and resilience requirements). A more comprehensive list has been written under D8.14’s section 6.3.

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

They take into account many levels of data security in an organisation. The requirements are general by their nature, and therefore, similarly to the above-mentioned GDPR's list of requirements, the data security measures listed in D8.14 should be read as recommendations, which should be implemented when they are applicable.

Also, the Article 28(3)(f) GDPR states that the Data Processing Agreement (or other legal act) shall stipulate that the processor assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36, taking into account the nature of processing and the information available to the processor. Thereby, the responsibility of implementing data security measures lies in both the controller's and processor's hands.

According to the EDPB's guidelines 07/2020 on the concepts of controller and processor in the GDPR (version 2.0, p. 37), the degree of detail of the information as to the security measures to be included in the contract must be such as to enable the controller to assess the appropriateness of the measures pursuant to Article 32(1) GDPR. Accurate descriptions are also essential in order for the controller to comply with the requirements concerning accountability stated in Article 24, and, respectively for the processor, in Article 28(3)(f) and (h), to assist the controller and to make available all information necessary.

In the aforementioned guidelines, it is also stated that the level of instructions provided by the controller to the processor as to the measures to be implemented will depend on the specific circumstances. Due to the nature of the SHAPES project, the controllers mainly do not provide accurate technical instructions. In most of the situations, the processor provides the controller with a service for which the technical measures have already been planned. Nevertheless, the measures have been deemed adequate, and their detailed descriptions can be easily found in the event any legitimate need arises. The processors are aware of the sensitiveness of the data to be processed.

As there are two separate official documents where the measures need to be described according to GDPR, it has been considered as the most practical option to compile a larger, collective data security document, where all of the data security measures implemented by the controllers and the processors can be viewed from. Another benefit of the document is that the processors, such as Digital Solutions, do not have to participate in every DPA and DPIA process when it comes to data security measures, and thus duplicate work can be avoided. The processors responsible for implementing data security measures merely describe their technical measures once in their own sections (and also any possible Use-Case-specific measures), and the pilot sites refer to those descriptions. The organisational measures are described by the pilot sites, after which, the referrals are made to the applicable sections containing the technical measures. Also, the security measures implemented for the SHAPES

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

platform are relevant for all the Pilot Sites and as such shall be described in its own section.

Using the collective document also makes it easier for the reader to acquire a more comprehensive understanding of implemented measures. It could be burdensome in practical situations where the need arises to find which measures have been implemented (and how), if, for instance, organisational measures had been written separately in DPIA documents. In that scenario, the reader would have to constantly jump between two documents, and ultimately, that could cause an infringement of the principle of transparency, which is established in Article 5(1)(a) GDPR. Also, Article 5(2) contains the basic rule for the principle of accountability, stating that the controller shall be responsible for, and be able to demonstrate, compliance with paragraph 1.

The more precise requirements concerning the principle of transparency are stated in Article 12, which is titled “Transparent information, communication and modalities for the exercise of the rights of the data subject”. Although Article 12 does not refer directly to Article 32 (security of processing), the transparency (and accountability) can be seen as a cross-sectional principle, which must be taken into consideration in all of the planned processing activities. Additionally, according to the EDPB’s guidelines 02/2021 on virtual voice assistants (p. 17), complying with the transparency requirement is imperative, since it serves as a control mechanism over the data processing and allows users to exercise their rights. Therefore, in a sense, the data security document can also be seen as an incarnation of the principles of accountability and transparency.

When it comes to the availability of the document, it has to be restricted as it will contain information that could be used for seeking any vulnerabilities in the chosen measures. Therefore, it will be accessible by the SHAPES partners and, if needed, on demand by supervisory authorities.

5.4 Transfers to third countries

As in certain Use Cases cloud services provided by, e.g., Google, will be utilised; the pilot sites have been instructed to list those entities within transfers to third countries in their DPIAs. Mostly, the major companies claim they abide by the GDPR (and therefore would not transfer data outside the EU/EEC in their own interest), but in practice many infringements have been seen. In his doctoral thesis, Wiatrowski (2021, 157) argues that even enormous fines have not stopped Google from acting how it pleases. Therefore, it is best to take that aspect into consideration and openly declare the services used.

Other currently known transfers outside of the EU/EEA in the SHAPES project are transfers into the UK, as described in chapter 3.1 (Data Processing Agreements), because some of the partners work under the UK jurisdiction, but also into Ukraine,

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

as there are parties that have joined the project through the open calls. It has to be noted that a duty rests on the data exporter to inform data subjects that it intends to transfer personal data to a third country or international organisation. According to the EDPB's guidelines 03/2020, on the processing of data concerning health for the purpose of scientific research, in the context of the COVID-19 outbreak, this includes information about the existence or absence of an adequacy decision by the European Commission. Hence, the pilot sites have been instructed to inform the data subjects about the recently adopted Commission implementing decision (C(2021) 4800 final) pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, but also the lack of such a decision when it comes to Ukraine. In these cases, the appropriate safeguards have to be verified in accordance with Article 46 GDPR, and most likely the standard contractual clauses (Commission Implementing Decision (EU) 2021/914) will be utilised.

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

6 Conclusion

The majority of the defined objectives for this deliverable have been reached. It could be said that the common thread between them has been defining obligations that the controllers and processors have to take into consideration before starting data processing activities. As for updating the data protection policy, it has to be performed after finishing this deliverable. The DPIA works of the pilots are still unfinished, and it would be good to have some results before assessing the need for an update.

One of the purposes set for this document was to give tools they can use to ensure and demonstrate that the data processing is compliant with privacy and data protection legislation, mainly with the GDPR. Along with the process of writing this deliverable, the templates for DPIAs and data processing agreements were created and adjusted for slightly different scenarios. Their functions have been explained in the previous sections. Instructing on how the data security measures are to be defined is closely related to both of these official documents, and by the time of writing this deliverable, the collective data security document has already gained many entries from the SHAPES partners.

Other set objectives that can be considered accomplished are describing the reasoning behind the chosen legal basis for data processing in Use Cases, and also addressing the transfers into third countries or international organisations. Consent being applicable to all the Use Cases is a simple solution. Utilising consent, it does not need to be assessed, whether the processing activities will be performed solely in the public interest.

The question concerning secondary use of personal data remains partially open, since it is being currently discussed Union-wide. Nevertheless, backgrounds for the current legal situation were presented along with the approximate schedule for the long-awaited supranational special legislation (lex specialis). It is important to acknowledge, that since the Council has encouraged the Commission to prioritise the European Health Data Space over the other data spaces, it is still possible to see the new regulation in place before the end of the project.

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

7 Ethical Requirements Check

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)	The right to privacy or private life is enshrined in the Universal Declaration of Human Rights (Article 12), the European Convention of Human Rights (Article 8) and the European Charter of Fundamental Rights (Article 7). The Charter contains an explicit right to the protection of personal data (Article 8).
Biomedical Ethics and Ethics of Care (3.2)	N/A
CRPD and supported decision making (3.3)	N/A
Capabilities approach (3.4)	N/A
Sustainable Development and CSR (4.1)	N/A
Customer logic approach (4.2)	N/A
Artificial intelligence (4.3)	Automatic decision making and profiling can rely on AI. In these situations, there must be a mechanism to guarantee the data subject's rights.
Digital transformation (4.4)	N/A
Privacy and data protection (5)	Referring to the objectives in section 1.2: provided templates for official documents required in GDPR; clarifying the situation of secondary use of personal data; clarifying the legal basis, explaining our risk assessment approach and, e.g., addressing the transfers into third countries.
Cyber security and resilience (6)	Mainly describing, how the measures will be described by the pilot sites (organisational measures) and technical partners (technical measures), and explaining the requirements imposed in the GDPR.
Digital inclusion (7.1)	N/A
The moral division of labour (7.2)	N/A
Care givers and welfare technology (7.3)	N/A
Movement of caregivers across Europe (7.4)	

Comments: _____

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

8 References

ARTICLE 29 DATA PROTECTION WORKING PARTY. (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679.

DG Health and Food Safety. (2021). *Assessment of the EU Member States' rules on health data in the light of GDPR.* Luxembourg: Publications Office of the European Union.

European Commission / DG SANTE. (n.d.). COMBINED EVALUATION ROADMAP/INCEPTION IMPACT ASSESSMENT / Ref. Ares(2020)7907993 - 23/12/2020.

European Data Protection Board. (2020). Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak.

European Data Protection Board. (2020). Guidelines 05/2020 on consent under Regulation 2016/679.

European Data Protection Board. (2021). Guidelines 02/2021 on virtual voice assistants.

European Data Protection Board. (2021). Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

European Data Protection Supervisor. (2020). A Preliminary Opinion on data protection and scientific research.

European Data Protection Supervisor. (2020). Opinion 3/2020 on the European strategy for data.

European Data Protection Supervisor. (2020). Preliminary Opinion 8/2020 on the European Health Data Space.

Groos, D., & van Veen, E.-B. (2020). Anonymised Data and the Rule of Law. *European Data Protection Law Review*, 1-11.

Korja, J. (2016). *Biometrinen tunnistaminen ja henkilötietojen suoja: Tutkimus biometristen tunnisteiden lainsäädännöllisestä asemasta.* Rovaniemi: University of Lapland.

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

Mondschein, C. F., & Monda, C. (2019). The EU's General Data Protection Regulation (GDPR) in a Research Context. In P. Kubben, M. Dumontier, & A. Dekker, *Fundamentals of Clinical Data Science* (pp. 55-71). Springer, Cham.

Mourby, M., Mackey, E., Elliot, M. J., Gowans, H., Wallace, S. E., Bell, J., . . . Kaye, J. (2018). Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law & Security Review*, 222-234.

Wiatrowski, A. (2021). *Abuses of Dominant ICT Companies in the Area of Data Protection.* Rovaniemi: University of Lapland.

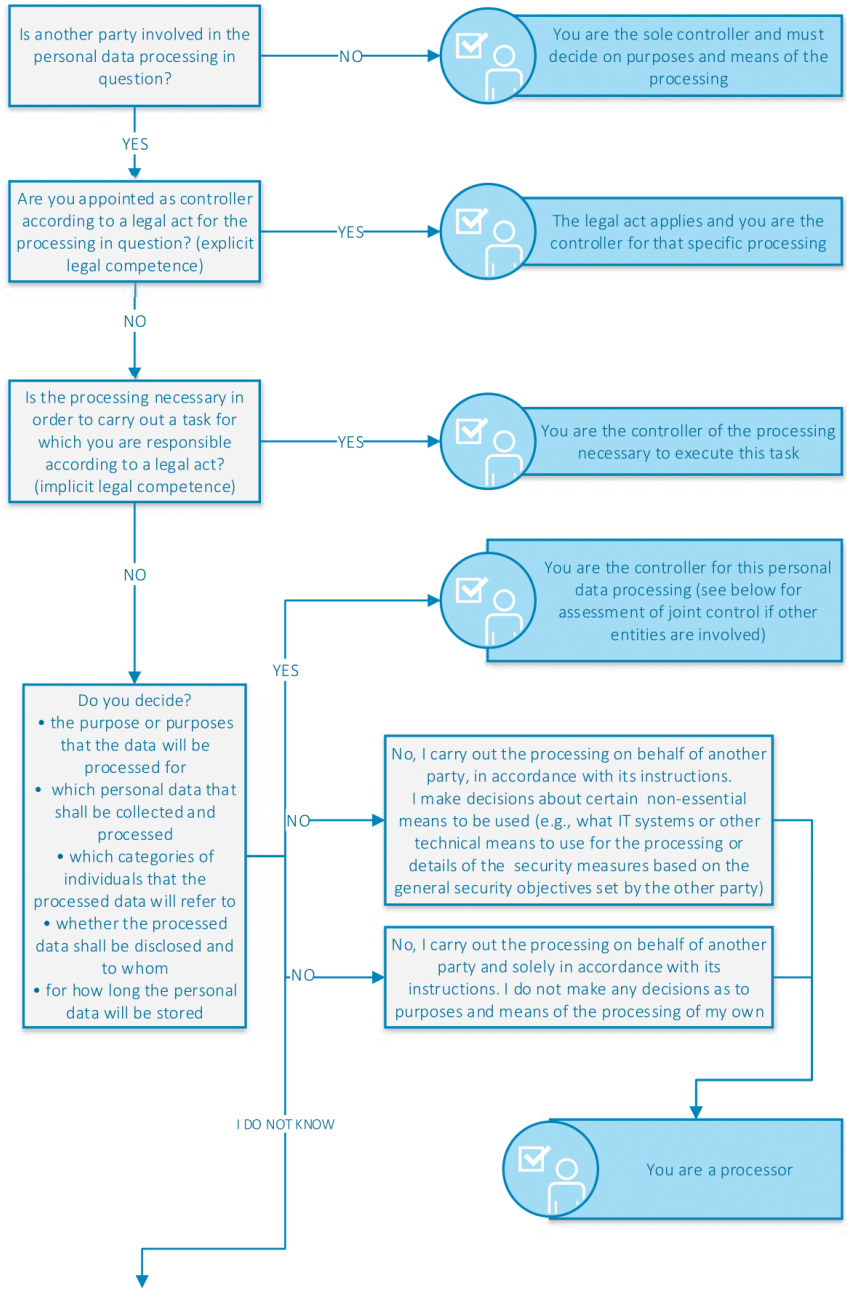
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159

Annex I

Source: European Data Protection Board. (2020). Guidelines 05/2020 on consent under Regulation 2016/679

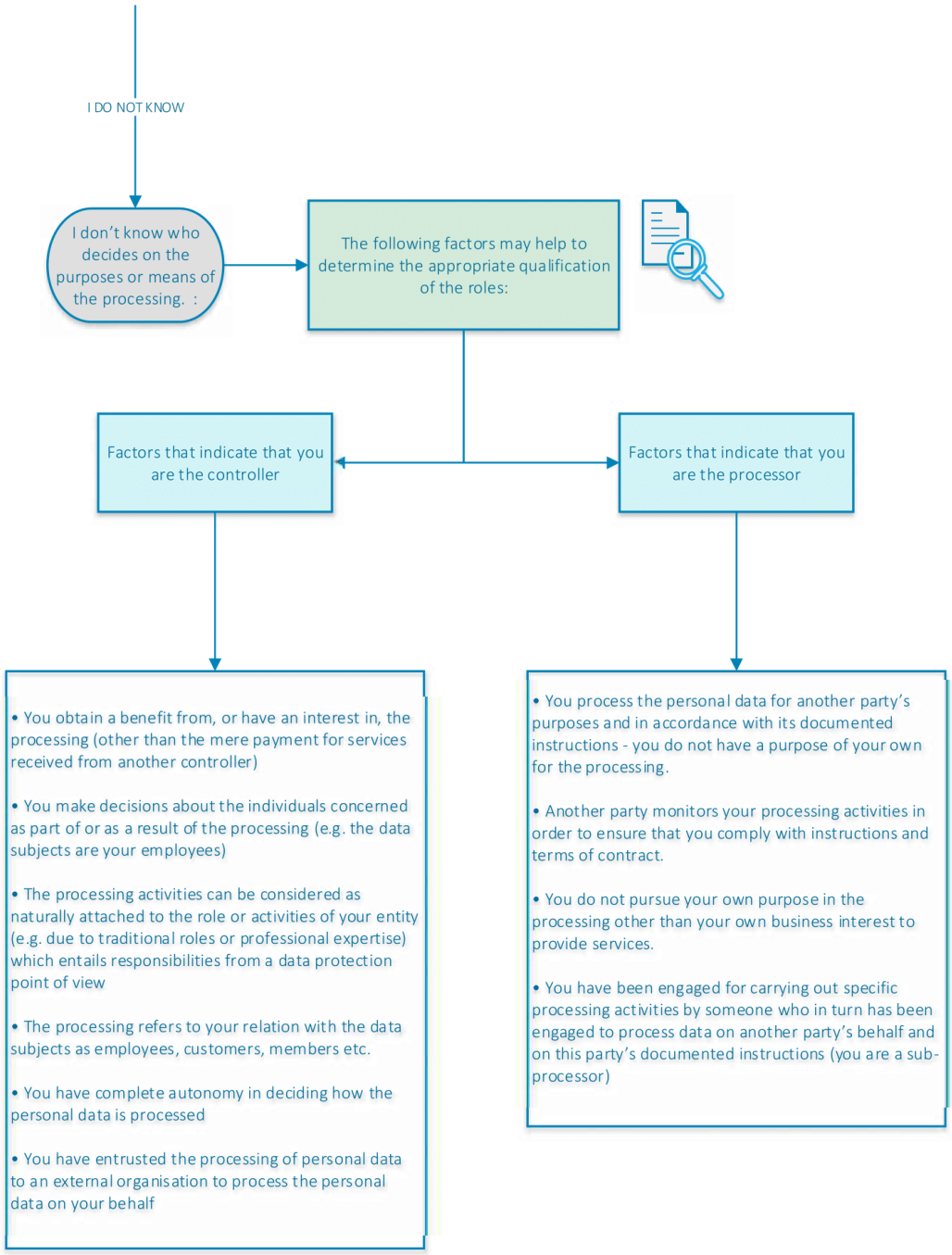
Annex I – Flowchart for applying the concepts of controller, processor and joint controllers in practice

Note: in order to properly assess the role of each entity involved, one must first identify the specific personal data processing at stake and its exact purpose. If multiple entities are involved, it is necessary to assess whether the purposes and means are determined jointly, leading to joint controllership.



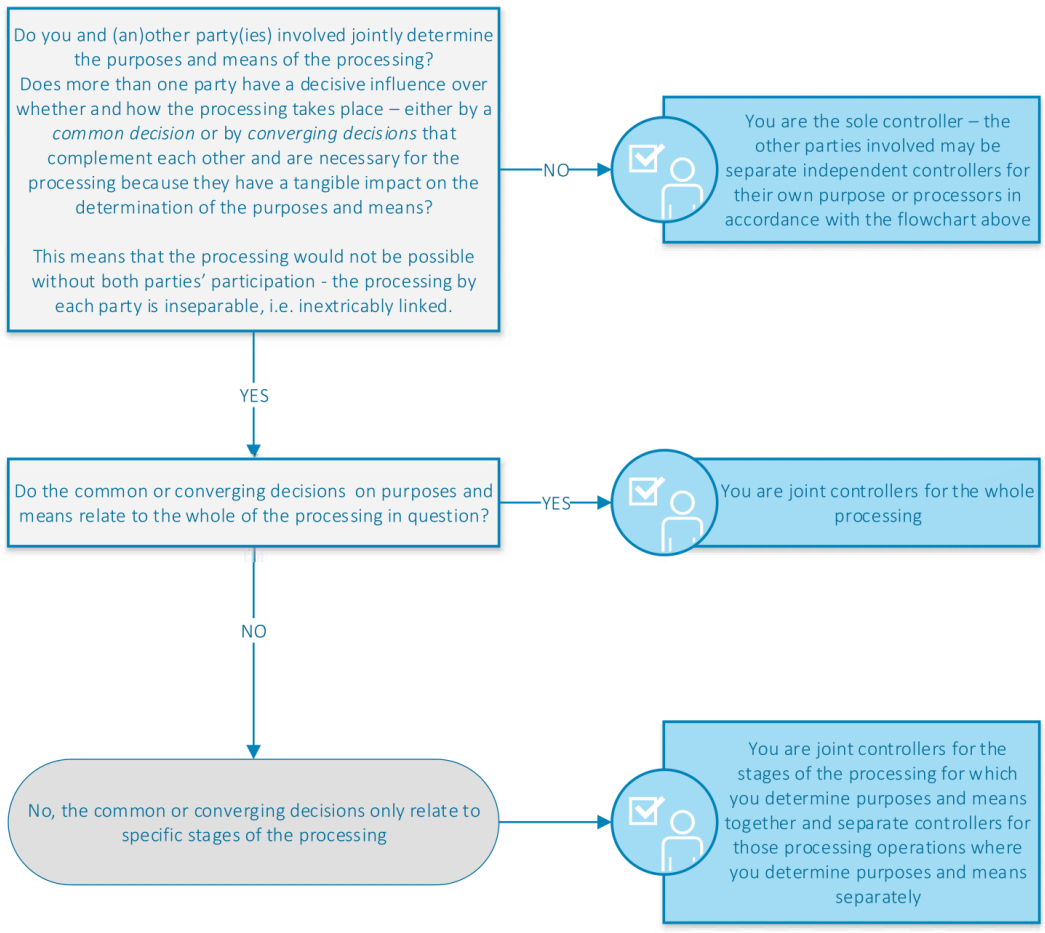
Adopted - version for public consultation 46

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



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

Joint controllership - If you are the controller and other parties are involved in the personal data processing:



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

Annex II

SHAPES Data Processing Agreement

ANNEX

Standard contractual clauses

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). The purpose is also to ensure compliance with Section 59(5) and (6) of the United Kingdom's Data Protection Act 2018 (c. 12), when relevant.

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725. The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance also with Section 59(5) and (6) of the United Kingdom's Data Protection Act 2018 (c. 12), when relevant.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725 and/or, when relevant, United Kingdom's Data Protection Act 2018 (c. 12).

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725 and/or, when relevant, Chapter 5 of the United Kingdom's Data Protection Act 2018 (c. 12).

Clause 2

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

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725 and/or, when relevant, United Kingdom's Data Protection Act 2018 (c. 12) or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 - Optional

Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

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

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II

OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law or, when relevant, United Kingdom law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State or, when relevant, United Kingdom data protection provisions.

7.2. Purpose limitation

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

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

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

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725 and/or, when relevant, United Kingdom's Data Protection Act 2018 (c. 12). At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a)

OPTION 1: PRIOR SPECIFIC AUTHORISATION: The processor shall not subcontract any of its processing operations performed on behalf of the controller in accordance with these Clauses to a sub-processor, without the controller's prior specific written authorisation. The processor shall submit the request for specific authorisation at least [SPECIFY TIME PERIOD] prior to the engagement of the sub-processor in question, together with the information necessary to enable the controller to decide on the authorisation. The list of sub-processors authorised by the controller can be found in Annex IV. The Parties shall keep Annex IV up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least [SPECIFY TIME PERIOD] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The

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

processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725 and/or, when relevant, United Kingdom's Data Protection Act 2018 (c. 12).

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

(c) "Onward transfers", which from the perspective of the United Kingdom controller or processor constitute international transfers from the United Kingdom, can be permitted only where the further recipient outside the United Kingdom is itself subject to rules ensuring a similar level of protection to that guaranteed within the United Kingdom legal order. Any such onward transfer shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the controller or the

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

processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 or Chapter 5 of the United Kingdom's Data Protection Act 2018 (c. 12).

Clause 8

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
(4) the obligations in Article 32 of Regulation (EU) 2016/679 and, when relevant, Section 66 of the United Kingdom's Data Protection Act 2018 (c. 12).

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

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

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725 and, when relevant, Sections 67 and 68 of the United Kingdom's Data Protection Act 2018 (c. 12), where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679 and, when relevant, Section 67(4) of the United Kingdom's Data Protection Act 2018 (c. 12), shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(2) the likely consequences of the personal data breach;
(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679 and, when relevant, Section 68 of the United Kingdom's Data Protection Act 2018 (c. 12), with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

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

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679 and, when relevant, Sections 67 and 68 of the United Kingdom's Data Protection Act 2018 (c. 12).

SECTION III

FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725 and/or, when relevant, the United Kingdom's Data Protection Act 2018 (c. 12), in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

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

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725 and/or, when relevant, the United Kingdom's Data Protection Act 2018 (c. 12);
(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725 and/or, when relevant, the United Kingdom's Data Protection Act 2018 (c. 12).

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I

List of parties

Controller(s): [Identity and contact details of the controller(s), and, where applicable, of the controller's data protection officer]

1.

Name: …

Address: …

Contact person's name, position and contact details: …

Signature and accession date: …

2.

…

Processor(s): [Identity and contact details of the processor(s) and, where applicable, of the processor's data protection officer]

1.

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

Name: …

Address: …

Contact person's name, position and contact details: …

Signature and accession date: …

2.

…

ANNEX II

Description of the processing

Categories of data subjects whose personal data is processed

…

Categories of personal data processed

[you can enter the same categories which you marked in the DPIA descriptions template]….

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

…

Nature of the processing

[as listed in GDPR, for instance collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction]
….

Purpose(s) for which the personal data is processed on behalf of the controller

[you can use the information you entered into descriptions template here too] …

Duration of the processing

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

…

…

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing

ANNEX III

Technical and organisational measures including technical and organisational measures to ensure the security of the data

EXPLANATORY NOTE:

The technical and organisational measures need to be described concretely and not in a generic manner.

Description of the technical and organisational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons. **Examples** of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

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

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller

[Description of the specific technical and organisational measures to be taken by the processor to be able to provide assistance to the controller]

ANNEX IV

List of sub-processors

EXPLANATORY NOTE:

This Annex needs to be completed in case of specific authorisation of sub-processors (Clause 7.7(a), Option 1).

The controller has authorised the use of the following sub-processors:

1.

Name: …

Address: …

Contact person's name, position and contact details: …

Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): …

2.

…

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

Annex III

The different data-protection-related tasks / documents in SHAPES

Actual processing of personal data starts (pilot goes live)

Before the processing starts

Agreements must be in place

2 to 3 months

DPIA must be ready

Data processing agreement (WORD)	Data processing descriptions (EXCEL)	Risk assessment (EXCEL)	DPIA Word Document
- Pilot site has to do this with every processor - Do not fill in the data security measures here, but instead refer to the relevant parts of the Data Security Document	- The processing operations are described - Purposes, transfers to third countries, legal basis, categories of personal data - All the processors and other stakeholders are listed	- Pilot site has to define risks for the Use Case - The collective risk document can be checked for ideas (every pilot site can fill in this document)	- Pilot site has to write this document by using the template - It is recommended to start filling in this template from paragraph 7 (Data Flow Chart), which helps identifying all the partners you need a data processing agreement with - Do not fill in the data security measures here, but instead refer to the relevant parts of the Data Security Document

The Data Security Document

Pilot sites describe their organisational security measures | Technical partners describe the technical data security measures

The Data Security Document and the Collective Risk Assessment Document can be found in the Maynooth Teams server's Pilots and DPO channel.

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

Annex IV

Class	No	Requirement	Importance	Responsibility before the project	Responsibility after the project	Processes	More information in D8.14 section
Ethical requirements for the governance, business and ecosystem models	GE23	Update and publish data protection and cybersecurity policies	Mandatory	WP8, WP10	Governance?		Privacy & DP, Cyber-security
General Ethical Requirements for the development	GE31 (GE32 - 36, GE40, GE46)	Conduct DPIA and ensure that the following data protection principles are embedded in the DPIA: lawfulness, fairness, transparency, purpose limitation, storage limitation, accuracy	Mandatory	WP5, WP6	Governance? Service provider	Service joins, Service development, Platform development	Privacy & DP
General Ethical Requirements for the development	GE24 (GE25 -30)	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	WP4, WP5, WP6	Governance? Marketplace? Service provider	Service joins, Service development, Platform development	Privacy & DP
General Ethical Requirements for the development	GE38	Automated decision making: if processing contains automated decision making, build a manual process to comply with art. 22 of GDPR.	Mandatory	WP6, WP5	Governance? Marketplace? Service provider	Service joins, Service development	Privacy & DP
General Ethical Requirements for the development	GE39	Privacy by design and by default: ensure data protection is taken into account when starting to plan for new services or processes. Adopt a “privacy first” approach.	Mandatory	WP4, WP5, WP6	Governance? Marketplace? Service provider	Service joins, Service development, Platform development	Privacy & DP
General Ethical Requirements for the development	GE41	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	WP6	Governance Service provider	Service joins, Service development, Platform development	Privacy & DP
General Ethical Requirements for the development	GE42	Technical and organisational security measures: identify and document who needs to have access to personal data.	Mandatory	WP6	Governance? Marketplace? Service provider	Service joins, Service development, Platform development	Privacy & DP
General Ethical Requirements for the development	GE45	Ensure that privacy and data-protection-related legal documents are in place (for example NDAs and data processing agreements).	Mandatory	WP6, WP7	Marketplace Service provider	Service joins, Service development, Platform development	Privacy & DP

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

Ethical requirements for user support processes	PE4 (PE5)	Provide training material on data protection and cybersecurity to end-users who need to understand data protection (older persons, caregivers, researchers).	Mandatory	WP8	Governance? Service provider	User joins, User uses	Privacy & DP, Cyber-security, Lifelong learning
Ethical requirements for user support processes	PE6	Provide a process for executing data subject rights in SHAPES.	Mandatory	WP8, WP6, other?	Marketplace? Governance, Service provider	User uses, user leaves	Privacy & DP
Ethical requirements for the SHAPES Technological Platform	ET4	Data subject rights: right of access – provide a self-service portal where the data subject can get access to his/her data.	Desirable	WP4, WP5	Marketplace, Service provider	Platform development, User joins, User uses	Privacy & DP
Ethical requirements for the SHAPES Technological Platform	ET5	Data subject rights: right to rectification – ensure that the data can be corrected in all places (incl. storage).	Mandatory	WP4, WP5	Marketplace, Service provider	Service development, Platform development, Service joins	Privacy & DP
Ethical requirements for the SHAPES Technological Platform	ET6	Data subject rights: right to be forgotten – build capabilities for deleting personal data.	Mandatory	WP4, WP5	Marketplace, Service provider	Service development, Platform development, Service joins, User leaves	Privacy & DP
Ethical requirements for the SHAPES Technological Platform	ET7	Data subject rights: right to restriction – build a capability for restricting data processing.	Mandatory	WP4, WP5	Marketplace, Service provider	Service development, Platform development, Service joins	Privacy & DP
Ethical requirements for the SHAPES Technological Platform	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	WP4, WP5, WP6	Marketplace, Service provider	Service development, Platform development, Service joins	Privacy & DP
Ethical requirements for the SHAPES Technological Platform	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	WP4, WP5	Marketplace, Service provider	Service development, Platform development, Service joins	Privacy & DP
Ethical requirements for the SHAPES Technological Platform	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	WP5	Marketplace, Service provider	Service development, Service joins, User uses	Privacy & DP

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

Ethical requirements for the SHAPES Technological Platform	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	WP4, WP5	Governance, Service provider	Service development, Platform development, Service joins	Privacy & DP
Ethical requirements for the SHAPES Technological Platform	ET12	Data protection principles: accuracy – ensure that the source of the data is recorded.	Mandatory	WP4, WP5	Governance, Service provider	Service development, Platform development, Service joins	Privacy & DP
Ethical requirements for the SHAPES Technological Platform	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	WP4, WP5	Governance, Service provider	Service development, Platform development, Service joins, User joins	Privacy & DP
Ethical requirements for the SHAPES Technological Platform	ET14	Create traceability capabilities for personal data; data mapping/data flows.	Mandatory	WP4, WP5	Governance, Service provider	Service development, Platform development, Service joins	Privacy & DP
Ethical requirements for the SHAPES Technological Platform	ET15	Automated decision making: Ensure that there is a capability to re-direct the decision to a manual process.	Mandatory	WP5	Governance, Service provider	Service development, Platform development, Service joins	Privacy & DP
Ethical requirements for the SHAPES Technological Platform	ET16	Privacy by design and by default: implement needed privacy enhancing technologies.	Mandatory	WP4, WP5	Governance, Service provider	Service development, Platform development, Service joins	Privacy & DP
Ethical requirements for the SHAPES Technological Platform	ET18	Personal data breach: create capabilities to identify potential personal data breaches	Mandatory	WP4, WP5	Governance, Service provider	Service development, Platform development, Service joins, User uses	Privacy & DP
Ethical requirements for the SHAPES Technological Platform	ET19	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	WP4	Governance, Service provider	Service development, Platform development, Service joins	Privacy & DP
Ethical requirements for the SHAPES Technological Platform	ET20	Keep logs for personal data (who has seen/modified personal data and when).	Mandatory	WP4, WP5	Service provider	Service development, Platform development, Service joins	Privacy & DP

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

Ethical requirements for the governance, business and ecosystem models	ME8 (ME9 - ME 11, GE40, GE46)	Establish privacy and data protection governance model for SHAPES - Roles and responsibilities - Data subject rights - DPIAs - Privacy information - Privacy policy	Mandatory	WP3, WP6	Governance	Privacy & DP

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

Annex V

Template of personal data processing descriptions
[Instructions: Copy this sheet to create the appropriate description for each service/pilot. After filling in the description, add the name and REF nbr to the 'Processing list' sheet. Store this file in the WPs teams Data Management / Data Protection folder].

Description of the processing operation	
Name of the processing operation	
Short description of research/service/pilot/other processing activity	
N° / REF	
Date of creation of the processing	
Update of the processing	

Stakeholders	Name	Address	Country	Phone number	Email address
Controller					
Data protection officer					
DPO's Organisation (if external DPO)					
Processor					
Joint controller(s)					

Purpose(s) of the data processing	Description	Legal basis
Main purpose		
Sub-purpose 1		
Sub-purpose 2		
Sub-purpose 3		
Sub-purpose 4		
Sub-purpose 5		

Source of personal data (if not from data subject)	Personal data categories / description	How is it confirmed that you're authorised to use such data for this purpose?		
Source 1	[add personal data categories received from third parties here]			
Source 2				
Source 3				
Categories of personal data	**Description**	**Special categories of personal data**	**Data retention period in years**	**Reasoning for data retention period**
Basic information				
Medical and Health				
Behavioural				
Financial				
Social				
Location				

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

Technical information				
Other?				

Categories of data subjects	**Description**	**Details**
Category 1		
Category 2		

Recipients (who has access to data)	**Type of recipient**	**Type of guarantees**	**Details**
Recipient 1			
Recipient 2			

Processing contains automated decision making	**Yes/No**	**Describe how data subjects' rights have been implemented**	**Link to material**

Service/processing uses profiling	**Yes/No**	**Legal basis for profiling**	**Can data subject object?**	**Link to material**
Description of profiling				

Security measures	**Type of security measure**	**Details**
Security measure 1		
Security measure 2		

Transfers to third countries or international organisations	**Recipient**	**Country**	**Type of guarantees**	**Legal basis for transfer**	**Frequency of the transfers**
Recipient organisation 1					
Recipient organisation 2					
Recipient organisation 3					
Recipient organisation 4					

Data storage	**Detailed description**	**Link to data map / architecture picture etc.**
Technical name 1		
Technical name 2		
Technical name 3		
Technical name 4		
How are data subjects informed on processing?	**Description**	

Link to the data protection related material						

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

Annex VI

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

S H A P E S

Project Title	**S**mart and **H**ealthy **A**geing through **P**eople **E**ngaging in supporting **S**ystems
Project Acronym	SHAPES
Project Number	857159
Type of instrument	Innovation Action
Topic	DT-TDS-01-2010
Starting date of Project	01/09/2019
Duration of the project	48
Website	TBD

Data Protection Impact Assessment (DPIA)

[Pilot xx]

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

[Date]

Dissemination level:

CO: Confidential, only for members of the consortium (including the Commission Services)

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

8.1.1.1 Version History

Revision	Date	Editor	Comments
0.1	DD/MM/YYYY	LAUREA	First version of the DPIA template
1.0	12.3.2021	LAUREA	Template ready for use

8.1.1.2 Table of Contents

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

1 Introduction to this DPIA

This DPIA is part of the SHAPES research activities and has been conducted before the pilots' personal data gathering starts. DPIA will consist of three different documents: Data processing descriptions, risk analysis and this SHAPES Pilot xx DPIA document. This document will form the assessment on whether the processing of personal data is on the right level from the GDPR point of view, and it will also describe the potential corrective actions that have been taken if the risk analysis has shown that there are some changes needed. Using this DPIA, the pilots can also assess whether they've implemented all ethical requirements for privacy and data protection set in SHAPES D8.4.

This DPIA was prepared by XX

[Instructions: all sections contain examples and instructions – remove those from your final version.]

2 Short description of the [use case/pilot/other processing]

PILOT xx; name

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

[This can be taken from Personal Data Processing Descriptions document]

3 Purposes of data processing

[The main purposes can be taken from data processing descriptions. Describe what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, data subject and more broadly?

Remember that in this document you need to justify the collection of the personal data especially from data subjects' point of view.]

4 Context of the processing

[You can use the questions below to describe the context.

- What is the nature of the relationship with the individuals – e.g. do you already know them, are they existing customers?
- How much control will they have over their data?
- Would they expect you to use their data in this way?
- Is it data which people are likely to consider particularly 'private'?
- Do they include vulnerable groups?
- Are there prior concerns over this type of processing or security flaws?
- What is the current state of technology in this area (are you building up something new or using existing technology – do you use it in a different way than before)?
- Are there any current issues of public concern that should factor in?]

This project has received funding from the European Union's Horizon 2020 research and innovation programme

under grant agreement No 857159

5 Necessity and proportionality

[Describe how this processing helps to achieve the purpose – Why it is necessary to collect the information you've planned? You can use the questions below to formulate your answer:

- Is there another way to achieve the same outcome?
- Can you achieve the same purpose without the processing?
- Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?]

[Describe how the pilot will ensure data quality and data minimisation?]

6 Ensuring data subjects' rights

A link to the document where the data subject's rights in the SHAPES pilots are described will be inserted here.

7 Data flows

[Describe how and from where you will receive the data, where the data is stored and will the data be transitioned or transferred to third parties. It would be good to use a data flow diagram or similar].

8 Description of the automated decision making

[Describe the automated decision making if it will be used in this pilot/service. Automated decision making means that a decision that affects the individuals somehow is made without a human.]

This project has received funding from the European Union's Horizon 2020 research and innovation programme

under grant agreement No 857159

9 Profiling

[Describe what kind of profiling this pilot/use case conducts? How has it been ensured that there will not be errors? What kind of safeguards are in place? How will the transparency be ensured?]

[Profiling is the automated processing of personal data for evaluating personal aspects. Example:

Imposing speeding fines purely on the basis of evidence from speed cameras is an automated decision-making process that does not necessarily involve profiling. It would, however, become a decision based on profiling if the driving habits of the individual were monitored over time, and, for example, the amount of fine imposed is the outcome of an assessment involving other factors, such as whether the speeding is a repeat offence or whether the driver has had other recent traffic violations.

A simple classification of individuals based on known characteristics, such as their age, sex and height, does not necessarily lead to profiling. If an organisation merely wants to classify their customers for statistical purposes without making predictions or drawing any conclusion about an individual, it is not considered profiling.]

10 Security measures

[Add a description here of the security measures taken on the pilot site and in this use case. In addition, add a link to the SHAPES Security document, which describes how the security has been arranged in the SHAPES platform].

11 Risk assessment

[Add the end-result of the risk assessment done for this pilot/use case here.]

This project has received funding from the European Union's Horizon 2020 research and innovation programme

under grant agreement No 857159

12 Conclusions and agreed actions

[Add a conclusion of the DPIA - are all data processing activities at the right level? Do you see a risk for the data subjects? If there were some risks that need to be followed up or issues that still require action, describe those here.]

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

Annex VII

Risk assessment template

Risk identification						Risk analysis		Risk impact and propability				Risk management actions				
Risk identification nbr	Risk classification		Root cause	Risk (name)	Consequences	Probability	Impact	Risk significance (P x I)		Need for mitigation actions		Proposed actions for risk		Description for mitigationactions in place + planned	Responsible person	Schedule
	1	Privacy	*New way of using data *Surveillance systems used	Information collection might be seen intrusive				0	Not assessed	0	Not assessed	0	Not assessed			
	2	Security		Loss/ uninteded modification of data				0	Not assessed	0	Not assessed	0	Not assessed			
	4	Other		Unintended causes to individuals (specify)				0	Not assessed	0	Not assessed	0	Not assessed			
	1	Privacy		Inability to use individual rights				0	Not assessed	0	Not assessed	0	Not assessed			
	1	Privacy	Consent information not adequate	Loss of control over the future use of personal data				0	Not assessed	0	Not assessed	0	Not assessed			
	2	Security	*Human error *Security breach	Identity revealed				0	Not assessed	0	Not assessed	0	Not assessed			
	3	Data management	*Data retention period not set *No process for removing data according to set timeframes	Information will be used for longer than necessary				0	Not assesse	0	Not asses	0	Not assess			

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

Annex VIII

Privacy Notice/Policy for SHAPES research data

If you don't process personal data during this research study, you can leave this appendix out. Please note that the information sheet regarding the use of the SHAPES platform will be provided later on.

Within the SHAPES project, your personal data will be processed according to the European Union General Data Protection Regulation and current national regulation. The processing of personal data will be described in the following items.

Data controller of the SHAPES project

[The data controller is the natural or legal person, public authority, agency or other body who alone or jointly with others determines the purposes and means of the processing of personal data].

Write the name of the data controller: organisation name and address.

If there are two or more controllers who jointly determine the purposes and means of processing personal data as part of this research, they are joint controllers. Describe the roles and the division of responsibilities between the parties here.

Contact person for matters related to the processing of personal data

Provide the name, email address and phone number of the contact person for matters related to the processing of personal data.

Types of personal data that will be collected in this study

Provide all of the personal data and personal data types you will process. If necessary, you can use a separate appendix. Personal data can be, e.g., a name, a personal identity code, an email address that contains a real name, facial data, voice data, fingerprints, the iris of an eye, the shape of a palm, a traditional signature, an address, a phone number, an IP address, a student identification number, an insurance number, an account number, detailed income information, a given title such as a chairmanship, gender, age, home municipality, profession, place of study, specific dates (date born, date died, time of an

This project has received funding from the European Union's Horizon 2020 research and innovation programme

under grant agreement No 857159

event) as well as sensitive data (race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health data, sexual orientation etc.).

Describe whether personal data will be collected from other sources; for example, from official registries. What kind of data will be collected and on what basis?

Personal data protection principles

Describe the information systems, software, applications etc. used for collecting and processing personal data.

Describe how the information systems have been protected. *For example, as in the following*:

The data that is to be processed in the information systems has been protected using the following:

user ID ☐ password ☐ user registration ☐ access control (physical location) ☐

If other methods, please specify:

For what purpose will personal data be processed?

Please write a short description of the purpose of the study.

Legal basis of processing personal data

Please enter the same legal basis as you have provided in the privacy notice.

In scientific research, the legal basis is usually a task carried out in the public interest.

You have the right to withdraw the consent at any time as described in this notice.

Nature and duration of the study completed within the SHAPES project (how long the personal data will be processed):

One-time research ☐ Follow-up research

Duration of the research:

This is the time frame needed for collecting and analysing the data and for the publication

This project has received funding from the European Union's Horizon 2020 research and innovation programme

under grant agreement No 857159

of the study (plus three years for possible reclamations about the research results and time needed to respond).

What happens to the personal data after the study within the SHAPES project has ended?

Please describe the measures to be taken at the end of the study regarding whether the personal data will be destroyed or archived and for how long. *For example, as in the following*:

How the personal data will be processed after the study has ended:

If any research materials containing personal data will be destroyed

If any research materials containing personal data will be archived

without identifiers

with identifiers

Where the materials will be archived and for how long:

Data transfer outside of the research registry:

Please describe whether personal data will be transferred outside the research group (to whom and for what purpose). Please also take into account possible transfers to data processors (for example translators).

Possible transfer of personal data outside the EU or the EEA:

Please describe if data will be transferred to a third country. For example: Your data will not be / will be transferred outside of the EU or the EEA.

If yes, specify the data to be transferred, the purpose and the object of the transfer, as well as the legal basis for the transfer in line with the GDPR.

Your rights as a data subject

Because your personal data will be used in the study taking place within the SHAPES project, you will be entered into the study registry. Your rights as a data subject are the following:

This project has received funding from the European Union's Horizon 2020 research and innovation programme

under grant agreement No 857159

Of the following two options, please choose the one that is in line with your processing basis and delete the extra text. It is sufficient to enter a list of the rights and to mention how they can be exercised. [N.B. Add open data]

If your *processing basis is a task carried out in the public interest*, please list the following rights:

- Right to obtain information on the processing of personal data
- Right of access
- Right to rectification
- Right to restriction of processing
- Notification obligation regarding rectification of personal data or restriction of processing
- Right to object to the processing
- Right not to be subject to a decision based solely on automated processing
- Right to notify the Data Protection Ombudsman if you suspect that an organisation or individual is processing personal data in violation of data protection regulations.
- You can exercise your rights by contacting the data controller of the study.

If your *processing basis is consent granted by the data subject*, please list the following rights:

- Right to obtain information on the processing of personal data
- Right of access
- Right to rectification
- Right to erasure (right to be forgotten)
- Right to withdraw consent regarding processing of personal data
- Right to restriction of processing
- Notification obligation regarding rectification or erasure of personal data or restriction of processing
- Right to data portability
- The data subject can allow automated decision making with his or her specific consent
- Right to notify the Data Protection Ombudsman if you suspect that an organisation or individual is processing personal data in violation of data protection regulations.

If the purposes for which a controller processes personal data do not or no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this regulation. If the controller cannot identify the data subject, the rights of access, rectification, erasure, notification obligation and data

This project has received funding from the European Union's Horizon 2020 research and innovation programme

under grant agreement No 857159

portability shall not apply, except if the data subject provides additional information, enabling his or her identification.

You can exercise your rights by contacting the data controller of the study.

Personal data collected in the SHAPES project for research will not be used for automated decision making. In the SHAPES project studies, the processing of persal data is never used in any decisions concerning the participants of the research.

Pseudonymisation and anonymisation

Please modify the next two chapters to suit your study and delete the unnecessary parts:

All information collected from you will be handled confidentially and according to the legislation. Individual participants will be given a code, and the data will be stored in a coded form in the SHAPES project files. Results will be analysed and presented in a coded, aggregate form. Individuals cannot be identified without a code key. A code key, which can be used to identify individual research participants and their responses, will be stored (by whom), and the data will not be given to people outside the SHAPES-project study group. The final research results will be reported in aggregate form, and it will be impossible to identify individual participants. The SHAPES project study registry will be stored (where) for (XX) years, after which it will be destroyed (please describe how). (Or alternative method).

The SHAPES professionals must inform participants if the collected data will be used for later research (for example, "The data collected from you can be later... The participant has the right to request information of people who have received data for their use…"). If the legal basis for processing personal data has been consented, and you wish to use the data in further studies, a specific consent for that must be obtained. Please mention if you intend to cooperate internationally and clarify the confidentiality and protection of the data as well as possible agreements on data processing.

This project has received funding from the European Union's Horizon 2020 research and innovation programme

under grant agreement No 857159