D1.7 Ethics Data Processing Activities Risk Evaluation

WP1– Project Management

Version: 1.00

SPHINX

A Universal Cyber Security Toolkit for Health-Care Industry

Disclaimer

Copyright message

Document information

Grant Agreement Number	826183	Acronym	SPHINX

Full Title	A Universal Cyber Security Toolkit for Health-Care Industry			
Topic	SU-TDS-02-2018 Toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures			
Funding scheme	RIA - Research and Innovation action			
Start Date	1st January 2019	**Duration**	36 months	
Project URL	http://sphinx-project.eu/			
EU Project Officer	Reza RAZAVI (CNECT/H/03)			
Project Coordinator	Dimitris Askounis, National Technical University of Athens - NTUA			
Deliverable	D1.7 Ethics Data Processing Activities Risk Evaluation			
Work Package	WP1 – Project Management			
Date of Delivery	**Contractual**	M9	**Actual**	M9
Nature	R - Report	**Dissemination Level**	P - Public	
Lead Beneficiary	VUB-LSTS			
Responsible Author	Dimitra Markopoulou	**Email**	Dimitra.Markopoulou@vub.be	
	Vagelis Papakonstantinou		Evangelos.Papakonstantinou@vub.be	
		Phone		
Reviewer(s):	Evangelos Stamatiadis (DYPE5), Fotios Gioulekas (DYPE5), Konstantinos Gounaris (DYPE5), Athanasios Tzikas (DYPE5), Ricardo Cabecinha (HES)			
Keywords	Ethics, Data Processing, Risk Assessment			

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Document History

Version	Issue Date	Stage	Changes	Contributor
0.10	18/07/2019	Draft	ToC	Dimitra Markopoulou (VUB-LSTS) / Vagelis Papakonstantinou (VUB-LSTS)
0.20	08/9/2019	Draft	Draft report for internal review	Dimitra Markopoulou (VUB-LSTS) / Vagelis Papakonstantinou (VUB-LSTS)
0.30	20/09/2019	Draft	Review 1	Evangelos Stamatiadis (DYPE5), Fotios Gioulekas (DYPE5), Konstantinos Gounaris (DYPE5), Athanasios Tzikas (DYPE5)
0.40	20/09/2019	Draft	Review 2	Ricardo Cabecinha (HES)
0.50	25/09/2019	Pre-final	Incorporated review comments, submitted for QC	Dimitra Markopoulou (VUB-LSTS) / Vagelis Papakonstantinou (VUB-LSTS)
0.51	30/09/2019	Pre-final	Quality Control	Michael Kontoulis (NTUA)
1.00	30/09/2019	Final	Final	Christos Ntanos (NTUA)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Executive Summary

This deliverable report constitutes an evaluation of the ethics risks posed by personal data processing within the SPHINX project context. To this end, its first part analyses in a general manner the ethics risks that are related to personal data processing in research. Findings of its first part are then particularised onto the SPHINX project circumstances in the second part. Finally, part three examines the need for conducting a DPIA within the SPHINX project – a question that this deliverable reports answers in the negative.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Table of Tables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

1 Ethics risks related to the processing of personal data in research; When is a data protection impact assessment necessary?

1.1 Introduction. How to identify ethics risks related to the processing of personal data in research

Protection of personal data is a fundamental human right and at the same time a major ethical issue when research ethics are being considered. Processing of personal data in research may raise ethical concerns if such processing is not conducted in full compliance with ethical and legal requirements (ethical principles and the General Data Protection Regulation – Regulation (EU) 2016/679, the "GDPR").

As far as research ethics in particular are concerned, safeguarding the privacy of research subjects and protecting their personal information should be the main ethic concern researchers need to address when their research involves processing of personal data. Research subjects' rights, when processing of their personal information takes place, should be respected throughout the research. Therefore, during all stages of research, as appropriate, data subjects should be provided with detailed information regarding any parameter of processing of their personal data, for instance what data are being collected, for what purpose, how long will they be stored for, will they be destroyed if no longer needed, who is the processor and his contact details, how the data subject can have access to such data, has the data subject given its free, explicit consent for the processing, is the data subject informed about his/her right to be forgotten or the right to withdraw consent regarding such processing etc.

The importance of protection of one's privacy and the potential risks the violation of such privacy may entail, makes safeguarding this right a major concern for anyone involved in research. This concern is even greater when special categories of data (health data, data regarding religion) or data concerning children or vulnerable groups of people are being processed, as well as when complex processing of personal data takes place (a large-scale processing, big data processing). All these are issues that should be identified, evaluated and addressed in all research projects funded by the EU.

How could compliance with research ethics be achieved though? The first step would be to identify and evaluate the ethics risks that data processing in the specific research may entail. Once this is completed, next step includes adopting the right measures to address such risks and ensure ethical and legal compliance. In other words, minimisation of ethics risks, as well as of their potential negative impact on research subjects, could be achieved through the conduct of an ethics risks assessment. How should the risk assessment be organised and implemented will be examined in the following sections.

1.2 The European Commission's approach towards ethics and the processing of personal data in EU-funded research

EU is seeking high levels of assurance with regard to data processing and ethics in all research projects it intends to fund. In this context, the European Commission has published guidance on how to complete and ethics self-assessment addressed to all EU funding applicants.[1] In these guidelines, which aim to help applicants in getting their proposals ethics-ready, the Commission suggests that an ethics risk assessment should be conducted by all applicants, with data processing being one of the issues that needs to be addressed when considering possible ethical implications. In addition to these guidelines, the Commission has issued a report entitled ethics

[1] https://ec.europa.eu/research/participants/data/ref/fp7/89888/ethics-for-researchers_en.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

and data protection. This document also aims to assist applicants to address any data protection issues in their research proposal and ultimately ensure compliance. Finally, the Commission has released the European Textbook on Ethics in research[2] which focuses mainly on key ethical issues that may appear in scientific research and, in particular, research that involves human beings. The fourth chapter of this study refers to privacy and confidentiality and more specifically their role in research ethics.

The Commission's effort to clarify, to the best extent possible, the ethics concerns that may be raised during research, as well as to motivate researchers to this effect, indicates the importance of conducting research ethically.

1.3 What are the main ethics issues that need to be addressed in research that involves the processing of personal data?

Processing of personal data should always be conducted lawfully and in an ethical manner. Controllers and when applicable processors should always be ready to verify compliance with the applicable legislation and take the appropriate measures to safeguard data subjects' privacy and other rights directly related to the processing of their personal data. This is the general rule that applies to any personal data processing. There are however some parameters which, when occurring, raise extra ethics concerns for researchers/controllers. These parameters are examined below in the sections that follow.

1.3.1 Processing of special categories of data

According to article 9 par.1 of the GDPR special categories of personal data include personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or a natural person's sex life or sexual orientation. In more detail, article 4 of the GDPR provides the following definitions:

- **genetic data** : that means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
- **biometric data**: that means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data; and
- **data concerning health**: that means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Processing of these categories of data is prohibited under the GDPR. There are exceptions to this rule that are listed in article 9 par.2. Some of the exceptions include the data subject's explicit consent to the processing, protection of vital interests of the data subject, processing is necessary for the exercise or defence of legal claims etc.

In terms of research in particular, article 9 par 2 (j) states that processing of special categories of data shall not be prohibited in case processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR. The last article reads as follows:

[2] https://ec.europa.eu/research/science-society/document_library/pdf_06/textbook-on-ethics-report_en.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

"Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner".

Given that processing of these categories of data during research is likely to raise significant ethics issues, some of them being discrimination against data subjects, stigmatization, exposing identity and sensitive data etc, it is suggested that such processing should always be justified. Taking into consideration this risk and the Regulation's provisions on this matter, any researcher/controller, whose research involves processing of special categories of data should be able to demonstrate that:

- Extra protective safeguards are in place;
- Processing of special categories of data is allowed as it falls within one of the exceptions of article 9 par 2 of the GDPR;
- The data are relevant and limited to the purposes of the research project;
- Informed consent has been acquired;
- Anonymization/pseudonymisation techniques are in place;
- Security measures shall be implemented.

1.3.2 Processing of personal data concerning children and vulnerable people

Children as data subjects always raise serious concerns when ethics and compliance with ethical principles are being considered. As per recital 38 of the GDPR children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.

As far as vulnerable groups of people are concerned these are defined as groups that include captive populations (prisoners, institutionalised, students etc), mentally ill persons, aged people, children, critically ill or dying, poor, with learning disabilities, sedated or unconscious. Sometimes vulnerable participants are understood as those who are unable to give valid consent either due to lack of competence or because of circumstances which cast doubt upon its voluntariness. One of the most explicit accounts is that of the Council for International Organizations of Medical Sciences, which defines vulnerable persons as *"those who are relatively (or absolutely) incapable of protecting their own interests"*. The key elements however in all these definitions is that the vulnerable person is at higher risk of harm or exploitation than others would be in a similar situation and/or is less able than others to protect themselves from harm or exploitation.

Given the higher risk processing personal data of children and vulnerable people may entail, particular levels of care will be required from controllers in order to confirm compliance with the General Data Protection Regulation. The best way to do that is by acquiring consent and make sure that such consent is not imposed indefinitely on these groups rather than re asked (for instance for children when the reach legal majority). Consent as the lawful basis for processing a child's or a vulnerable person's personal data could not however be the sole possible solution. Sometimes using an alternative basis may prove better in terms of safeguarding the children's rights.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

With regard to children in particular, GDPR establishes special safeguards for them in relation to "information society services". These include a requirement for verified parental consent in respect of information society services offered directly to children aged under 16. Individual Member States may provide for this threshold to be lowered to 13 years. In this context, controllers must be aware of the age of consent in particular Member States. Informed consent will be thoroughly examined below under the relevant section.

What should be pointed out here and with regards to these special groups of people is that researchers should make an effort to

- include such participants in their research only when this is absolutely necessary;
- make sure, to the extent possible, that the people who are legally responsible for them have sufficient information that allows them to make the informed consent choice on their behalf and in their best interests. Article 8(2) particularly adds that *"The controller shall make reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology";*
- Make the content of informed consent understandable to the child by using a language that is clear and plain for children.

1.3.3 Complex processing operations (processing of personal data on a large scale, monitoring of a publicly accessible area on a large scale) - Invasive data processing techniques (profiling, data mining, privacy invasive methods or technologies)

In all cases where research involves large scale processing of personal data or invasive data processing techniques or techniques that may be used for surveillance, tracking or profiling, additional ethics concerns and implications should be taken into consideration.

a. Automated processing, including profiling

The GDPR includes specific safeguards for automated processing or profiling of personal data. A definition of profiling is included in article 4 (4) of the Regulation according to which profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Article 22 of the GDPR regulates automated individual decision-making, including profiling. Par. 1 of article 22 sets the data subject's right not to be subject to a decision based solely on automated processing. Par. 2 lists three exceptions to this rule (the decision is necessary for the performance of a contract, the subject has given its explicit consent, the decision is authorised by Union law). If this is the case the controller is obliged to implement suitable measures to safeguard the subject's rights, such as specific information to the data subject and the right to obtain human intervention.

b. Data processing on a large scale

The GDPR does not include a separate article for large scale processing of personal data. However, several references to this type of processing are found in the Regulation's body. More specifically, processing on a large scale of special categories of data, as well as a systematic monitoring of a publicly accessible area on a large scale are types of processing that are likely to result in a high risk to the rights and freedoms of natural persons. Therefore, the Regulation provides for additional safeguards to be implemented by the controller whose core

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

activities include this kind of processing. In particular, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (article 35). Furthermore, this type of processing burdens the controller with the additional obligation to designate a data protection officer (article 37).

1.3.4 Collecting or transferring data outside the EU

Collecting or transferring data outside the EU is another ethical issue that needs to be addressed in order to ensure that data subjects' rights are protected, when this type of data processing takes place.

Transfers of personal data to third countries (or international organisations) is regulated under article 44 of the GDPR. The article reads as follows: *"Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined".* Under EU law one way to transfer personal data abroad is on the basis of a Commission "adequacy decision" establishing that a non-EU country provides a level of data protection that is "essentially equivalent" to that in the EU. The "adequacy" criterion is introduced in article 45 of the GDPR: a transfer of personal data to a third country may take place where the Commission has decided that the third country in question ensures an adequate level of protection.

In the event that such Commission's decision does not exist, article 46 of the Regulation provides that a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Such safeguards include standard contractual clauses (SCCs) and binding corporate rules (BCRs). The Commission has so far issued two sets of standard contractual clauses for data transfers form data controllers in the EU to data controllers established outside the EU, as well as one set of contractual clauses for data transfers form controllers in the EU to processors established outside the EU.[3] As far as BCR are concerned these include internal rules for data transfers within multinational companies.[4]

In this context transfer of data outside the EU needs to be identified and specified in each research project. At the same time the handling process of such data transfers should be specified.

The ethics and data protection report published by the Commission report refers that few non-EU countries have received an 'adequacy determination' from the European Commission indicating that they have a data protection framework offering a level of protection equivalent to that provided under EU law.[5] The report lists the conditions that need to apply in order for data transfers to non-EU countries to be lawful, namely:

- the explicit consent of the data subject (which requires them to be informed in advance of any such transfers);

[3] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

[4] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en

[5] The list of countries covered by a Commission adequacy determination is available at: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacyprotection-personal-data-non-eu-countries_en

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

- an 'adequacy determination' by the European Commission in respect of the country in question;
- a data-transfer agreement containing EC standard contractual clauses giving effect to EU data protection law; or
- binding corporate rules covering both sender and recipient and approved by a national supervisory authority. These requirements apply to all personal data transfers, regardless of the sensitivity of the data.

In more detail prior to any transfer of data outside the EC Member States, researchers should make sure that the place where the data is to be sent has a data protection regime in place that is at least as solid as that required in the EU, or at least conform to the GDPR's requirements.

Same ethical concerns are raised when collecting personal data from subjects in non-EU countries is involved. If this is the case the controller/researcher should make sure that:

- Processing, notification, consent and accountability provisions meet GDPR standards;
- Identify any further data protection requirements in applicable laws in the country where data are collected;
- Ensure that research participants understand and consent to the export of their personal data;
- Use pseudonymisation or anonymisation techniques to minimise the risk to data subjects;
- Implement appropriate measures to ensure that personal data are transferred securely.

1.3.5 Informed consent

Informed consent is the cornerstone of research ethics. Both participation in research in the first place and collecting personal data from research subjects cannot be performed lawfully without the prior informed consent of the research/data subjects.

Acquiring informed consent from subjects participating in research is addressed in Deliverable D2.2. (ethical principles applicable to research). As far as informed consent in the context of GDPR is concerned, the notion is explicitly included and defined in the GDPR. Recital 32 of the GDPR states that consent should be given by a clear affirmative act establishing a freely given, specific informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him/her. Recital 42 defined informed consent as follows: For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Finally, article 7 lists the conditions for consent including the subject's right to withdraw such consent at any time.

By combining the above it is concluded that the basic requirements for a valid legal consent are the following:

- **Consent must be freely given.**

This entails a real choice by the data subject. Any element of inappropriate pressure turns the consent invalid. According to recital 42, consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

- **Consent must be specific and informed.**

The Commission sets the minimum elements the consent form should include in order for consent to be informed:

  - the identity of the data controller and, where applicable, the contact details of the DPO;
  - the specific purpose(s) of the processing for which the personal data will be used;
  - the subject's rights as guaranteed by the GDPR and the EU Charter of Fundamental Rights, in particular the right to withdraw consent or access their data, the procedures to follow should they wish to do so, and the right to lodge a complaint with a supervisory authority;

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

- information as to whether data will be shared with or transferred to third parties and for what purposes; and
- how long the data will be retained before they are destroyed.

- **Consent must be bound to one or several specified purposes**

Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them.

- **Consent must be unambiguous**

This means that consent requires either a statement or a clear affirmative act. Consent cannot be implied and must always be given through an opt-in, a declaration or an active motion, so that there is no misunderstanding that the data subject has consented to the particular processing.

As mentioned above under 3.2, research that involves children or vulnerable groups of people should be handled with extra caution in terms of acquiring consent.

1.3.6 Data security/confidentiality

a. What does data security involve?

The GDPR requires all data controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk faced by the data subjects in the event of unauthorised access to, loss, alteration deletion or destruction of their data. These measures include for instance:

- The pseudonymisation and encryption of personal data;
- The ability to ensure confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data;
- A process for regularly testing, assessing and evaluating the effectiveness of these measures.

Data security is also reinforced by the data breach notification process described in article 33 of the GDPR. The article states that in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority.

Finally, article 34 describes the procedure that needs to be followed by the controller when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons and needs therefore to be communicated to the data subject.

b. Evaluation of risk and adoption of security measures (the role of a risk assessment)

Data security is of the essence. When data processing is involved in a research project researchers (acting as data controllers or processors) should be always able to demonstrate that they have applied the appropriate technical an organisational measures to ensure security of the personal data they are processing for their research purposes (encryption of personal data, policies that ensure confidentiality and integrity of the processing systems etc.). This obligation is even more imperative when higher risk processing is taking place, like for instance processing that involves special categories of data or processing that may lead to profiling or large-scale processing etc.

The best way to move forward is of course through the conduct of a sound risk assessment. The level of data security must always be appropriate to the risks for the research participants occurring in case of unauthorized access or disclosure, accidental deletion or destruction of the data.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

ENISA has issued useful guidelines to this effect entitled Handbook on Security of Personal Data Processing.[6]

1.3.7 Keeping data processing lawful; Principles applicable to personal data processing

All ethics concerns developed in the previous sections fall under the general assumption that personal data processing is conducted in a lawful manner and that the data subjects' rights are being safeguarded throughout project execution.

a. Lawfulness of processing

Lawfulness of processing is the first principle that needs to apply when personal data are being processed. Art.5.1(a) of the EU GDPR states that*, "personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject"*. This principle of lawfulness of processing is further defined in its Article 6, where it is stated that *"processing of personal data shall be lawful only if and to the extent that at least one of the following applies:*

(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks". Consequently, the principle of lawfulness of the processing requires that one of the above legal bases is used for the processing of personal data.

b. The principle of transparency

Article 5.1(a) of the EU GDPR discussed above, introduces also **the principle of transparency** Recital 39 further explains what transparency entails: *"[…] It should be transparent to natural persons that personal* data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.

c. The principle of purpose limitation and data minimisation

Two other principles that should always be respected when personal data undergo processing are the principle of purpose limitation and the principle of data minimization. The former dictates that personal data should be collected for specified, explicit and legitimate purposes. In this context further processing that is incompatible with the purposes already notified to the data subjects is not allowed. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are excluded.

With regard to data minimisation, this principle implies that personal data that are processed, should always be adequate, relevant and limited to the purposes for which they are processed.

c. The principle of accountability

[6] https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Finally, **the principle of accountability** is introduced by article 5 (2) of the Regulation. This principle requires that the controller shall be responsible for, and be able to demonstrate compliance with all principles related to data processing, namely:

- the principle of lawfulness, fairness and transparency;
- the principle of purpose limitation;
- the principle of data minimisation;
- the principle of accuracy;
- the principle of storage limitation.

1.3.8 Safeguarding data subjects' rights during research: Basic data subjects' rights

a. The right to information

The right of information is directly connected to the principle of transparency and is regulated in two articles, namely Articles 13 and 14. Distinction is made between cases where the information was obtained from the data subject and other cases. In this context, article 13 regulates the case where personal data have been collected form the data subject whereas article 14 lists the information to be provided to data subject where personal data have not been obtained from the data subject.

b. The right of access

This right occupies Article 15 in the Regulation, according to which the data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and specific information such as the purpose of the processing, the recipients to whom the data have been or will be disclosed, the right to request rectification etc.

c. The right to erasure (right to be forgotten) and the right to object

Article 17 of the Regulation grants individuals the right to have their personal information deleted by data controllers if specific conditions listed in its paragraph 1 are met (points a–f), among which is the withdrawal of consent. The right to object is laid down in Article 21 of the Regulation. In particular, par. 1 of article 21 reads as follows*: "The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims".*

1.4 Evaluating ethics concerns in research that involves personal data processing

As already mentioned above, compliance with research ethics could be achieved through the conduct of an ethics risk assessment. This assessment would include identification and evaluation of the ethics risks data processing in the specific research may entail and of course adoption of the right measures to address such risks and ensure ethical and legal compliance.

The importance of conducting an ethics self-assessment has been acknowledged by the European Commission in its guidance published in February 2019, entitled how to complete your ethics self- assessment.[7] These guidelines should be read together with the more specific guidance the Commission has issued regarding ethics and data protection.[8] Both documents provide assistance to researchers during the preparation of their project proposal and of course during its execution. An ethics self-assessment step by step has also been published by

[7] See http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

[8] See http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

the European Research Council established by the European Commission. Protection of personal data is again one of the main ethical issues that is included in the ethics issues table checklist provided for under the ERC report.[9]
The conduct of the ethics risk assessment and particularly the part that relates to the ethical concerns and risks personal data processing in research may entail, shall indicate whether a data protection impact assessment is necessary for the research in question. This issue is analytically examined below under section 5.

1.5 Data protection impact assessment

1.5.1 When is it necessary?

A data protection impact assessment is a process designed to describe the data processing taking place, assess the necessity and proportionality of such processing and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data. Data protection impact assessment is regulated under article 35 of the GDRP. As per par. 1 of said article " Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. Paragraph 3 of article 35 indicates the cases where a data protection impact assessment shall in particular be required, that is:

a. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person
b. processing on a large scale of special categories of data referred to in article 9(1), or of personal data relating to criminal convictions and offences referred to in article 10; or
c. a systematic monitoring of a publicly accessible area on a large scale

In other words, the GDPR does not require a DPIA to be carried out for every processing operation which may result in risks for the rights and freedoms of persons. It is only mandatory when such risk is considered high. This high risk is usually anticipated when new technologies are used or automated processing or processing on large scale is taking place or a systematic monitoring of a publicly accessible area on a large scale (see also recitals 89 and 91 of the GDPR). The WP29 clarifies that this list in a non-exhaustive list. There may be "high risk" processing operations that are not captured by this list, but yet pose similarly high risks. In this context it has produced a longer list of scenarios in which it is likely to be necessary to conduct a data protection impact assessment. The list is included in the Article 29 WP guidelines entitled "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". Based on this assumption the WP29 recommends in its guidelines that, where it is not clear whether a DPIA is required, a DPIA is carried out nonetheless as a DPIA is a useful tool to help data controllers comply with data protection law.
Consequently, if one combines both the GDPR article 35 and the guidelines issued by Article 29 WP it is concluded that carrying out a DPIA is not mandatory for every processing operation but is only required when processing is likely to result in a high risk to the rights and freedoms of natural persons. The special conditions under which a DPIA must be conducted, the processing operations that are subject to a DPIA and application of these to the SPHINX research project shall be examined below under the relevant section 3.

1.5.2 How to carry out a DPIA?

According to recital 90 of the GDPR a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk. The DPIA is updated throughout each project, therefore it could be started even if some of the processing activities have not yet been decided or predicted. Carrying out a DPIA is a continual process, not a one-time exercise.

[9] See https://erc.europa.eu/sites/default/files/document/file/EthicsSelfAssessmentStepByStep.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

A DPIA is carried out by the controller. Article 35 (2) of the GDPR mentions that the controller shall seek the advice of the data protection offices where designated, when carrying out a data protection impact assessment. This is also indicated by article 39 which lists among the tasks of the DPO the monitoring of the DPIA performance.
Carrying out the DPIA may be done by someone else, inside or outside the organization, but the controller remains ultimately accountable for that task.
According to article 35(9) performing a DPIA could be an interactive procedure. Where appropriate the controller shall seek the views of the data subjects or their representatives on the intended processing.
The WP29 provides some further clarification son this interactive relationship. In particular it considers that: - those views could be sought through a variety of means, depending on the context (e.g. an internal or external study related to the purpose and means of the processing operation, a formal question to the staff representatives or trade/labour unions or a survey sent to the data controller's future customers); - if the data controller's final decision differs from the views of the data subjects, its reasons for going ahead or not should be documented; - the controller should also document its justification for not seeking the views of data subjects, if it decides that this is not appropriate.
As far as the role of the processor in this process is concerned, article 28.3(f) states that the DPIA must be carried out with the processor's help, taking into account the nature of the processing and the information available to the processor.
With regard to the features a DPIA should include the GDPR sets out the minimum set of features in article 35(7), and recitals 84 and 90 respectively. As per article 35 these are:

- a description of the envisaged processing operations and the purposes of the processing;
- an assessment of the necessity and proportionality of the processing;
- an assessment of the risks to the rights and freedoms of data subjects;
- the measures envisaged to address the risks and to demonstrate compliance with the Regulation.

In addition to the abovementioned article 35 (7), recital 90 states that impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.
Generally speaking, the GDPR provides data controllers with flexibility to determine the structure and form of the DPIA they will decide to carry out. As the WP29 points out whatever the DPIA's form is, a DPIA must be a genuine assessment of risks, allowing controllers to take measures to address them.
The WP29 has proposed a list of criteria that should apply in order for a DPIA complies with the GDPR's provisions. These criteria can be used to show that a particular DPIA methodology meets the standards required by the GDPR. This list has been included in this report and includes the following elements:

1. A systematic description of the processing is provided (Article 35(7)(a)):

- nature, scope, context and purposes of the processing are taken into account (recital 90);
- personal data, recipients and period for which the personal data will be stored are recorded;
- a functional description of the processing operation is provided;
- the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;
- compliance with approved codes of conduct is taken into account (Article 35(8)).

2. Necessity and proportionality are assessed (Article 35(7)(b)):

- measures envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account:
- measures contributing to the proportionality and the necessity of the processing on the basis of:
    - specified, explicit and legitimate purpose(s) (Article 5(1)(b));
    - lawfulness of processing (Article 6);
    - adequate, relevant and limited to what is necessary data (Article 5(1)(c));
    - limited storage duration (Article 5(1)(e));

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

- measures contributing to the rights of the data subjects:
    - information provided to the data subject (Articles 12, 13 and 14);
    - right of access and portability (Articles 15 and 20);
    - right to rectify, erase, object, restriction of processing (Article 16 to 19 and 21);
    - recipients;
    - processor(s) (Article 28);
        - safeguards surrounding international transfer(s) (Chapter V);
        - prior consultation (Article 36).

3. Risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)):

- origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
    - risks sources are taken into account (recital 90);
    - potential impacts to the rights and freedoms of data subjects are identified in case of illegitimate access, undesired modification and disappearance of data;
    - threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
    - likelihood and severity are estimated (recital 90);
- measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);

4. Interested parties are involved:

- the advice of the DPO is sought (Article 35(2));
- the views of data subjects or their representatives are sought (Article 35(9)).

As a final safeguard the GDPR states that, when a DPIA reveals high residual risks, the data controller will be required to seek prior consultation for the processing from the supervisory authority (Article 36(1)). As part of this, the DPIA must be provided (Article 36(3)(e)).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

2 SPHINX and personal data processing. What data processing activities are expected to take place in the SPHINX project? What are the main ethics risks related to the data processing activities of the SPHINX project?

2.1 Personal data processing in the context of the SPHINX Project

The SPHINX project's purpose is to introduce a cybersecurity toolkit that will enhance the cyber protection of Health IT Ecosystem and ensure the privacy and integrity of the patients' data. The toolkit will be adapted or embedded on existing medical, clinical or health available infrastructures whereas the user will be able to select from a number of available security services through the SPHINX cybersecurity tool.

Given the above description, it could be assumed that the SPHINX solution will interfere with processing of personal data. Specifically, the embedment of the SPHINX toolkit in hospitals' infrastructures indicates that SPHINX may acquire, through its platform, access to patients' personal data (health data and other personal details). However, it should be pointed out that even in this case, SPHINX shall be the *processor* of the personal data. The controller shall always be the hospital and any other health infrastructure that will use the SPHINX solution.

With these parameters in mind, it could be assumed that personal data processing shall be conducted throughout the SPHINX project. Therefore, any ethical concerns such processing may raise should be evaluated. **It is pointed out that this report is drafted at an early stage of the SPHINX project and therefore includes preliminary argumentation and conclusions. Its purpose is to indicate the main ethical issues that data processing during the SPHINX project may raise. Accurate conclusions regarding possible complications as well as SPHINX's response to risks shall hopefully be derived through distribution to project partners of detailed questionnaires that will address these issues. Partner's responses shall contribute to accurately evaluate SPHINX's compliance with the GDPR requirements**.

2.2 Processing of special categories of data and of data concerning children and vulnerable groups in the SPHINX project

As mentioned above under 1.3.1, Article 9 par.1 of the GDPR includes, in the definition of special categories of personal data, data concerning health, namely personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. According to same article processing of these categories of data is prohibited under the GDPR with the exceptions referred to in par 2 of article 9. With regards to research in particular the Regulation includes a specific provision that allows processing of special categories of data in case processing is necessary, among others, for scientific purposes.

Taking into consideration SPHINX description and specifications it is concluded that any personal data processing during the project's lifetime will involve special categories of personal data and more particularly patients' health data. SPHINX solution shall be installed in hospitals' IT infrastructures and shall consequently have access to personal data of the hospitals' patients and employees. Such data may be further processed for the purposes of evaluating the threats and risks the hospitals are vulnerable to as well as in order to suggest and design the right solutions to address such risks.

Given that health data are by default associated with vulnerable groups of people (ill people for instance) and may of course refer to children (children hospitals) this ethical issue should also be evaluated in the SPHINX project.

Under these circumstances SPHINX should undertake extra precautions in order to address these concerns. Two parameters should however be taken into account. First that the SPHINX project is a research project and as such falls under the exception of article 9 par 2 (j) GDPR, and, second, that SPHINX, when it comes to personal

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

data processing, shall always be treated as a *processor* of personal data. Hospitals and health care centres that shall embed and use the SPHINX solution shall always serve as the data controllers.
Consequently, it is mainly the hospitals' obligation, as data controllers, to comply with the GDPR. Hospitals and health care providers should acquire informed consent form their patients and keep these forms updated, as applicable under their respective national data protection laws. With regard to the processing of patient's data for the SPHINX project purposes, hospitals should also include this further processing in their consent forms in order for the patients to be aware that their personal data may be processed for this purpose as well. Special treatment should be afforded to vulnerable groups of people and children (*Make the content of informed consent understandable to the child by using a language that is clear and plain for children, make sure, to the extent possible, that the people who are legally responsibility for them have sufficient information that allows them to make the informed consent choice on their behalf and in their best interests etc*.). SPHINX solution assumes that in all cases where processing of personal data is involved all lawful requirements at partner level have been implemented.
SPHINX as *processor* should undertake the necessary measures in order to comply with its own obligations under the GDPR. Most notably these include (indicative listing):

- Extra protective safeguards;
- Technical and organization measures for the protection of personal data;
- Acquire informed consent when necessary;
- The data are relevant and limited to the purposes of the research project;
- Anonymization/pseudonymisation techniques are in place;
- Security measures shall be implemented.

2.3 Complex processing operations (processing of personal data on a large scale, monitoring of a publicly accessible area on a large scale) – Invasive data processing techniques (profiling, data mining, privacy invasive methods or technologies)

As analysed above, under 1.3.3, the GDPR applies special measures as regards complex processing operations. These measures come in the format of either specific provisions (e.g. on profiling) or general requirements that are to be applied also in the case of complex personal data processing (e.g. DPIA). The increased risk for personal data set by this type of processing (profiling, data mining, processing on a large scale) justifies their special regulatory treatment. Ethical concerns are also directly connected with this type of risk, ultimately affecting the privacy, trust, safety and security of the individuals concerned.
However, as regards the SPHINX project such complex processing operations are not expected to take place, either during its development or during its deployment stage. SPHINX being aimed at constituting a cybersecurity tool, it is not based on the processing of personal data *per se* but is rather protective of such data. In addition, its development does not require the processing of large volumes of personal data, for example for validation or verification purposes. It is in this context that ethical or regulatory concerns on account of complex personal data processing are not anticipated in the SPHINX context.
Evidently, having said the above, project partners are and will remain alerted as to the risks posed by complex personal data processing operations. In the event that such occur, they will be instructed to address themselves to the Ethics and Security internal project boards, in order to deal with such matter accordingly.

2.4 Collecting or transferring data outside the EU

Transfers of personal data to third countries (or international organisations) is regulated under article 44 of the GDPR (see above under 1.3.4). Under EU law, one way to transfer personal data abroad is on the basis of a Commission "*adequacy decision*". The "*adequacy*" criterion is introduced in article 45 of the GDPR: a transfer of personal data to a third country may take place where the Commission has decided that the third country in question ensures an adequate level of protection.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

With regard to the SPHINX project in particular, an accurate evaluation on whether collecting or transferring of data outside the EU takes place will be demonstrated in the relevant deliverable (D7.2 & 7.6) where the SPHINX use cases will be legally assessed.
At this point it suffices to mention that all pilots participating in the SPHINX project are located in countries that are members of the EU (Greece, Romania and Portugal). Therefore, no extra measures should be undertaken in the context of the project's execution.
In the same context, ethical concerns are raised when collection of personal data from subjects in non-EU countries is involved. If this is the case, then the controller/researcher should make sure that/to:

- Processing, notification, consent and accountability provisions meet GDPR standards;
- Identify any further data protection requirements in applicable laws in the country where data are collected;
- Ensure that research participants understand and consent to the export of their personal data;
- Use pseudonymisation or anonymisation techniques to minimise the risk to data subjects;
- Implement appropriate measures to ensure that personal data are transferred securely.

2.5 Informed consent

The ethical issue of informed consent has been critically analysed above in section 1.3.5. In this section it is repeated that the SPHINX solution and platform shall have access to personal data of the hospitals and health centres patients and employees. Therefore, it should always be ensured that a valid consent form of the data subjects is in place. In the event of patients in particular, given that the data that may be processed are categories as special categories of data, additional precautions should be undertaken, as these are provided under the GDPR. Acquiring informed consent is the health care providers' obligation (hospitals, care centres and regional health authority) as data controllers. SPHINX could in particular, in cooperation with the hospitals, suggest the update of the informed consent form in order to include the specific purpose for which the patients' personal data may be processed, namely the personal data processing for the purposes of the SPHINX project.

2.6 Data security/confidentiality

a. General
The GDPR includes in its articles 32-34 an indicative list of measures the controller and the processor need to implement in order to ensure a level of security of processing that is appropriate to the risk. Some of these measures, include:

a) the pseudonymisation and encryption of personal data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Article 33 describes the notification process to be followed by the data controller when a data breach occurs. Finally, security is completed with the process of article 34 of the Regulation, namely the communication of a personal data breach to the data subject.
This set of obligations set the template under which data controllers and occasionally data processors should operate in order to comply with their obligation to keep the data they are processing secure.
Confidentiality of personal data is directly connected to security of processing. Once security is assured, personal data will be kept confidential.
b. How does security of processing apply to SPHNIX
The SPHINX ecosystem aims to assist health care institutions in their effort to minimize cybersecurity threats and to respond to cybersecurity incidents. As a security by design solution SPHINX serves (by default) the security of data processing. SPHINX solution's purpose is focused on safeguarding the security, integrity and

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

confidentiality of the personal data processed by hospitals and health care institutions by offering tailored solutions adapted to the specific needs of the IT health sector.
It is therefore necessary that the SPHINX solution takes all technical security measures so as to warrant security of any processing of personal data that may occur during or by its use (for instance pseudonymisation and encryption of personal data). However, it is stressed that SPHINX is not a security compliance tool; Instead, it is designed to operate as an additional security tool in an environment that is, supposedly, fully compliant with security and GDPR obligations. Having said that, hospitals and health care organisations that will use the SPHINX solution, must perform a risk assessment and adopt and implement any organisational and technical measures in order to ensure the confidentiality, integrity and availability of their processing systems and services. The sensitive nature of the personal data that are processed by these organisations, turn their obligation for security of a vital importance.
Consequently it is assumed that the SPHINX solution is designed on the basis of the "security by design" principle, however it is also designed based on the assumption that the health care organisations that will embed the SPHINX solution in their systems shall be fully compliant in terms of security both of their networks and accordingly of the personal data they collect, store and further process.
In any case the specific organisational and technical measures that needs to be undertaken as far as SPHNIX processing activities are concerned must be directly associated to the specific processing activities that will indeed take place. Other that the basic security measures referred to in articles 32-34 of the GDPR that applies to all cases where personal data processing takes place, in the case of SPHINX additional measures are expected to be implemented. To this effect a set of questionnaires (as the one included in this deliverable report) shall be distributed to project partners and based on the results it is anticipated that a set of specific technical and other measures will be presented as suitable and accordingly will apply in practice.

2.7 Lawfulness of the processing activities in the SPHINX Project

a. Lawfulness of processing/acquiring consent

Any personal data that may be processed by the SPHINX platform should be processed lawfully. In order for that to apply in practice SPHINX is depending on hospitals' and health care centres' compliance with their obligations as processors of personal data as these (obligations) derive from the GDPR. The obligation of processing data lawfully is more important given the sensitive nature of the data the hospitals and accordingly the SPHINX ecosystem will process. In this context, hospitals and health care centres that are using the SPHINX solution must always have an active and updated personal data protection policy that will safeguard that the data subjects – in this specific case, their patients - are always informed about the processing of their personal data and have provided their explicit consent for such processing. As mentioned above processing is considered lawful when one of the conditions mentioned in article 6 of the GDPR applies. Even though it's the hospitals' obligation to apply the appropriate legal basis in order for any processing they conduct to be lawful, informed consent of the data subjects that would include a specific reference of the additional purpose of processing of the data subjects personal data, namely for SPHINX to operate, would be a solution. Of course, SPHINX could provide hospitals with all necessary technical information and other details in order to make such consent informed, accurate and complete.

b. The principle of transparency

According to article 12(1) of the GDPR it is the controller's obligation to warrant transparency of processing. In particular the article reads as follows: "*The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means*".
Given that the SPHINX solution applies to hospitals and health care providers in general, it is their obligation, as data controllers, to warranty transparency of the processing of their patients' personal data. It is advised that hospitals and health care centres apply a data protection policy in order to be able at any time to provide

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

the data subjects with the required information regarding their personal data, as these are included in articles 13 and 14 of the GDPR.
With regard to SPHINX's processing activities, SPHINX relies on hospitals compliance with their obligation for transparency. In addition to that and in the event that SPHINX indeed processing personal data it is anticipated that the principle of transparency will be respected at all times.

c. The principles of purpose limitation and data minimisation

As far as SPHINX is concerned it is advised that the hospital that will use the SPHNIX toolkit complies with the principles referred above. Given that hospitals and health infrastructures process sensitive data, they should always apply an updated data protection policy and have an appointed DPO. With regard to purpose limitation in particular, it could be suggested that further processing that takes place for the purposes of the SPHINX project shall be compatible with the initial purposes for which the personal data of the patients and the hospitals' personnel, have been collected by the hospitals in the first place. This assumption is based on article 5 (b) of the GDPR that has been elaborated above under 1.3.7. In any case it is advised that hospitals follow their national rules on personal data protection compliance, and, if applicable, update their informed consents in order to include such processing purpose in them as suggested above under 2.7 (a). With regards to data minimization SPHINX should apply the necessary technical and organisational measures in order to ensure respect for the principle of data minimisation. As for the SPHINX toolkit itself it should be designed in such a way that the data processing principles will be implemented in practice in the event that any personal data should be processed. The data protection by design and by default principles are examined below under 2.9.

d. The principle of accountability of article 5 (2)

According to Article 5.2 of the GDPR, "*the controller shall be responsible for and be able to demonstrate compliance with paragraph 1 [the basic personal data processing principles]*". Consequently, it is the task of the data controller, in this case, the hospital/health care centre using the SPHINX Platform and toolkit, to take the necessary measures within its organization in order to be able to demonstrate both to the individuals concerned and to any future controls by the Data Protection Authorities that the data protection legislation has been observed. A data protection impact assessment, as well as the appointment of a data protection officer are obligations the hospitals need to comply with. SPHINX in particular should be able to demonstrate that data processing principles are respected. Whether a DPIA in the context of the SPHINX project needs to be performed is addressed below under Section 3.

2.8 Rights of the data subjects in the context of the SPHINX project

a. The right to information

The SPHINX project relies on the assumption that the hospitals and health care providers using the SPHINX solution, in their capacity as data controller, apply national laws and regulations for the purpose of personal data protection compliance, particularly, wherever applicable, inform in advance the data subjects/patients of the basic information referred to in article 13, such as its contact details (as controller) and, where applicable, of its representative, the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing, the recipients or categories of recipients of the personal data, if any etc. Other information, according to paragraph 2 of Article 13 would be the period for which the personal data will be stored, the existence of the right to request access to the data or erasure, the right to withdraw consent at any tome etc. In the event that further processing of personal data takes place in the SPHINX project, SPHINX's contact details should always be available to any persons that may be concerned. SPHINX should always be in position to inform such persons whether any processing of their personal data is conducted and if yes for what purposes.

b. The right to access the data

The right of access occupies Article 15 in the Regulation, according to which the data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and specific information such as the purpose of the processing, the recipients to whom the data have been or will be disclosed, the right to request rectification etc.
In the context of SPHINX, the hospital or health care centre, as data controller, must inform the data subjects/patients that their personal information are being processed, provide the data subject with the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

information of article 15 mentioned above as well as with a copy of the personal data undergoing processing, if requested (as per article 15(3)). In the event that any personal data processing takes place during the SPHINX project, it is anticipated that SPHINX shall be ready to provide such information and access to the data subjects or the hospitals in case they need to prove compliance.

c. The right to erasure (right to be forgotten) and the right to object

Article 17 of the GDPR grants individuals the right to have their personal information deleted by data controllers if specific conditions listed in its paragraph 1 are met (points a–f), among which is the withdrawal of consent. The right to object is laid down in Article 21 of the Regulation. In particular, par. 1 of article 21 reads as follows: "*The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims*".

In the SPHINX case, subject to national law deviations, hospitals and health care providers, as data controllers, should always be ready to provide the patient/data subject with the right to be forgotten and the right to object. If any of the conditions of par 3 of article 17 applies, the hospital should be able to keep the personal data in its records. Given that the data in question are health data the exemption of article 17(3) c reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3) could apply. SPHINX could fall under the exception of article 17(3)d on the grounds that any personal data processing in the SPHINX project is considered necessary for scientific research purposes. In such case SPHINX should of course be able to demonstrate that the right to be forgotten is likely to render impossible or seriously impair the achievement of the objectives of that processing.

2.9 The SPHINX solution and data protection by design

a. General

Recital 78 of the GDPR states that the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. These principles are regulated under article 25 of the Regulation which reads as follows: *"Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects".*

Par. 2 of the same article states that "*The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons*".

b. How these principles apply to SPHINX

SPHINX is a security solution that targets the health IT ecosystem. As such it should, at the early stage of its "architectural building", take the appropriate measures in order to implement the data protection by design and by default principles. It should, in particular, make sure that only personal data that are necessary for each specific purpose of the processing are processed, that they are stored for a specific time, that data subjects may easily exercise their rights as these are provided under the GDPR etc. Compliance with such principles will be further elaborated as the project evolves as well as when the evaluation of SPHINX business model takes place.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

2.10 Self risk-assessment questionnaire

Following the Commission's guidelines regarding ethical compliance, it is recommended that a self-risk assessment is performed in the context of SPHINX concerning the subject matter analysed in this report.
The questionnaire that follows could be used as a guidance by the SPHINX partners in order to minimise any chance of unethical personal data processing activities being conducted in the project's lifetime.

	Self risk-assessment questionnaire **Please answer the following questions with regard to your involvement and/or work on the SPHINX project**	**YES**	**NO**
1	Does your processing operation involve a large volume of individuals' and/or personal data?		
2	Does your processing involve special categories of data (e.g. health data, genetic data, biometric data)?		
3	Do you process personal data of children (younger than 16 years old) or of vulnerable groups of people?		
4	Do you apply invasive data processing techniques (profiling, data mining)?		
5	Do you collect or transfer data outside the EU?		
6	Do you use informed consent forms? Do you update such forms regularly?		
7	Are privacy requirements proactively built into the software/system code (privacy by design)?		
8	Are security and privacy features of the system enabled by default (privacy by default)?		
9	Do you apply a security policy for the protection of personal data against accidental or unlawful destruction, loss or alteration?		
10	Is such policy documented?		
11	Is such policy reviewed regularly especially after the occurrence of a breach?		
12	Is the policy communicated to all employees?		
13	Is the processing of personal data performed by an undefined number of employees?		
14	Can unauthorized individuals access the personal data processing system?		
15	Are the roles of personnel with access to personal data clearly defined?		
16	Are individuals with access to personal data bound by a confidentiality obligation?		
17	Are data processors (e.g. contractors, outsourcing) involved in data processing?		
18	If yes, do you apply guidelines for data processors?		
19	Do data processors apply a notification process to the controller?		
20	Are access rights allocated to the right persons?		
21	Are there common user accounts?		
22	Is there a specific password policy?		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

23	Do you implement effective backup and recovery mechanisms for personal data?		
24	Are these backups protected?		
25	Are the backed up personal data stored encrypted?		
26	Do you have a business continuity plan?		
27	Are you able to restore availability and access to data in a timely manner in case of an incident?		
28	Can users deactivate security settings?		
29	Do you provide users with the right to access their data?		
30	Do you have a privacy policy accessible by the users?		
31	Do you provide users with the right to object to processing of their data?		
32	Do you provide users with the right to ask for their data to be deleted?		
33	Do you provide users with the right to correct their data?		
34	Do you have an appropriate mechanism for obtaining data subject's consent?		
35	Is such consent freely given? Is your request to consent presented in a clear and plain language?		
36	Do you use pre-checked (opt-in) boxes?		
37	Do you provide users with the right to withdraw their consent at any stage of processing?		
38	Do you provide users with the ability to export a copy of the data collected in an intelligible format?		
39	Is the purpose of processing accurately defined?		
40	Are the data you collect proportionate to the purpose of processing?		
41	Do you store data for longer than it is required?		
42	Do you use an encryption mechanism to protect stored personal data?		
43	Do you destroy data at the end of the period of retention?		
44	Do you apply pseudonymisation and/or encryption of data?		
45	Do you have a DPO?		
46	If you do not have a DPO, do you have a person in charge for privacy matters to whom the data subject may address request?		
47	Do you have an incident response plan?		
48	Do you implement a cooperation policy with the competent authorities?		
49	Do you have adequate documentation to verify the above?		
50	Do you support accountability (e.g. have in place auditing mechanisms)?		
51	Do you implement segregation of roles?		
53	Do you provide the option to the users to modify their privacy settings?		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

54	Do you implement strong privacy defaults (e.g. privacy settings are set by default to giving no consent for use of personal data)		
55	Have you performed a Data Protection Impact Assessment?		
56	Do you use Privacy Enhancing Technologies (PET)?		
57	Do you use encrypted communication channels for transferring any personal data?		

Table 1:Self Risk Assessment Questionnaire

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

3 Should a data protection impact assessment be conducted for the SPHINX Project?

3.1 General

In section 1.5 of this report it was elaborated that a data protection impact assessment (DPIA) is not required in all cases where personal data are being processed. According to article 35 the following conditions need to apply in order for a DPIA to be mandatory:

- a specific type of processing takes place in particular one that uses new technologies
- the processing has a special nature, scope and purposes
- the processing in question is likely to result in a high risk to the rights and freedoms of natural persons.

The first question therefore that needs to be answered in order to confirm the need or not for conducting a DPIA is whether the processing in question is likely to result in a high risk. If this answer receives a negative reply, then no DPIA is needed. If the answer is yes, the next question is whether the processing falls under one of the exceptions of article 35 (5) and (10). Again, if the answer is positive, no DPIA is requested. If it is negative a DPIA must be conducted.

Article 35 par 3 of the GDPR provides some examples when a processing is likely to result in high risks. Its list includes:

a. automated processing, including profiling

b. processing on a large scale of special categories of data referred to in article 9(1), or of personal data relating to criminal convictions and offences referred to in article 10; or

c. a systematic monitoring of a publicly accessible area on a large scale

As already mentioned above under 1.5, the WP29 clarified in its guidelines that this list in a non-exhaustive list. There may be “high risk” processing operations that are not captured by this list, but yet pose similarly high risks. To this effect the 29 WP has produced a longer list of scenarios in which it is likely to be necessary to conduct a data protection impact assessment on the grounds that the processing in question is likely to result in a high risk.

The criteria that should be taken into consideration are:

- Evaluation or scoring, including profiling and predicting, especially from “aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements”;
- Automated decision-making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing “legal effects concerning the natural person” or which “similarly significantly affects the natural person”;
- Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through “a systematic monitoring of a publicly accessible area”;
- Sensitive data: this includes special categories of data as defined in Article 9 (for example information about individuals’ political opinions), as well as personal data relating to criminal convictions or offences;
- Data processed on a large scale: the GDPR does not define what constitutes large-scale, though recital 91 provides some guidance. In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale: a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; b. the volume of data and/or the range of different data items being processed; c. the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

duration, or permanence, of the data processing activity; d. the geographical extent of the processing activity;

- Datasets that have been matched or combined, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject;
- Data concerning vulnerable data subjects (recital 75): the processing of this type of data can require a DPIA because of the increased power imbalance between the data subject and the data controller, meaning the individual may be unable to consent to, or oppose, the processing of his or her data;
- Innovative use or applying technological or organisational solutions, like combining use of fingerprint and face recognition for improved physical access control, etc.;
- Data transfer across borders outside the European Union, taking into consideration, amongst others, the envisaged country or countries of destination, the possibility of further transfers or the likelihood of transfers based on derogations for specific situations set forth by the GDPR. -When the processing in itself "prevents data subjects from exercising a right or using a service or a contract" (Article 22 and recital 91). This includes processing performed in a public area that people passing by cannot avoid, or processing that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract.

A DPIA is not required in the following cases:

- where the processing is not "likely to result in a high risk to the rights and freedoms of natural persons;
- when the nature, scope, context and purposes of the processing are very similar to the processing for which DPIA have been carried out. In such cases, results of DPIA for similar processing can be used;
- where a processing operation has a legal basis in EU or Member State law and has stated that an initial DPIA does not have to be carried out, where the law regulates the specific processing operation and where a DPIA, according to the standards of the GDPR, has already been carried out as part of the establishment of that legal basis (Article 35(10);
- where the processing is included on the optional list (established by the supervisory authority) of processing operations for which no DPIA is required (Article 35(5).

3.2 A DPIA is NOT REQUIRED in the case of the SPHINX processing activities

Taking into consideration the above analysis and SPHINX's description, the following conclusion is established regarding the need for conducting a DPIA for SPHNIX's processing activities.

It has already been demonstrated that any personal data processing during the project's lifetime will involve special categories of personal data and more particularly patients' health data. SPHINX solution shall be installed in hospitals' IT infrastructures and shall consequently have access to personal data of the hospitals' patients and employees. Such data may be further processed for the purposes of evaluating the threats and risks the hospitals are vulnerable to, as well as in order to suggest and design the right solutions to address such risks. However, any possible processing of health data for the SPHINX purposes will be conducted for incidental and secondary purposes and not focused on the patients' personal data, as such. As a result, processing that includes profiling of health data on large scale are not considered as possibilities. Consequently, any risk associated to processing of personal data that may be conducted during the project's lifetime is considered low. Furthermore, SPHINX could also fall under the exception of article 35(1) "*when the nature, scope, context and purposes of the processing are very similar to the processing for which DPIA have been carried out. In such cases, results of DPIA for similar processing can be used*". In the case of SPHINX, it is taken for granted that all hospitals and health care providers involved in the project have conducted a DPIA as they are obliged to by the General Data Protection Regulation. It is in this context that a, separate, DPIA exclusively for the SPHINX personal data processing is not considered necessary.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

4 Conclusion

This deliverable report begins with the examination of the ethics risks posed by personal data processing in research in a general manner. Topics that are of particular concern have been identified (indicatively, the processing of special categories of data or the processing of children's data) in an attempt to map the possible sources of ethics infringements. In the same context, specific types of processing that need to be carefully considered by project partners have been identified – among which, profiling or data mining, transfers in non-EU countries, security and confidentiality obligations or informed consent requirements and procedures.

The second part particularises findings of its first part onto the SPHINX project circumstances. Taking into account the project's specifications and description, the general recommendations of part one are made concrete in the SPHINX context. Project partners are advised to take special notice, and measures, as regards their personal data processing operations both conceptually (in terms of applicable principles) and in practice (as regards concrete regulatory requirements). A questionnaire aimed at a risk evaluation self-assessment has been drafted and will be distributed among partners in the same regard: Its completion will assist further ethics and legal compliance work for project purposes.

The final finding of this report refers to a, possible, DPIA for the SPHINX project. Taking into account applicable legal provisions and available guidance by EU bodies, this report advises that a DPIA is not necessary for project purposes.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Annex I: **References**

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Centre for Information Policy Leadership, GDPR Implementation In Respect of Children's Data and Consent

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf

Article 29 WP, Guidelines on Automated individual decision-making and profiling for the purposes of Regulation 2016/679

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

Article 29 WP, Guidelines on Consent under Regulation 2016/679

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Article 29 WP, Guidelines on Data Protection Impact Assessment (DPIA)

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

ENISA, Handbook on Security of Personal Data Processing

https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

European Commission, Ethical Review in FP7, Data Protection and Privacy Ethical Guidelines

https://ec.europa.eu/research/participants/data/ref/fp7/89827/privacy_en.pdf

European Commission, Ethics for Researchers, Facilitating Research Excellence in FP7,

https://ec.europa.eu/research/participants/data/ref/fp7/89888/ethics-for-researchers_en.pdf

European Commission, European Textbook on Ethics in Research

https://ec.europa.eu/research/science-society/document_library/pdf_06/textbook-on-ethics-report_en.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

What are the major ethical issues in conducting research? is there a conflict between the research ethics and the nature of nursing? Fouka G et al., Health Science Journal
http://www.hsj.gr/medicine/what-are-the-major-ethical-issues-in-conducting-research-is-there-a-conflict-between-the-research-ethics-and-the-nature-of-nursing.php?aid=3485

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.