D2.2 Ethical Requirements

WP2– Conceptualisation, Use Cases and System architecture

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	D2.2. Ethical Requirements			
Work Package	WP2 – Conceptualisation, Use Cases and System Architecture			
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):	Michael Kontoulis (NTUA), Ilias Lamprinos (ICOM)			
Keywords	Basis of Legal and Ethical Requirements			

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	15/09/2019	Draft	Draft ready for submission to internal reviewers	Dimitra Markopoulou (VUB-LSTS) / Vagelis Papakonstantinou (VUB-LSTS)
0.30	25/09/2019	Draft	Review 1	Michael Kontoulis (NTUA)
0.40	20/09/2019	Draft	Review 2	Ilias Lamprinos (ICOM)
0.50	26/09/2019	Pre-final	Incorporated review comments, submitted for QC	Dimitra Markopoulou (VUB-LSTS)/ Vagelis Papakonstantinou (VUB-LSTS)
0.60	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

Purpose of this report is the identification and analysis of the regulatory and ethical framework relevant to the SPHINX project. Its findings need therefore to be taken into account by all project partners while executing their tasks. SPHINX aims to introduce a universal cyber security toolkit that will enhance the cyber protection of Health IT Ecosystems and ensure patients' data privacy and integrity. The SPHINX toolkit will be adapted or embedded on existing medical, clinical or health available infrastructures. In the context of the project, SPHINX's cyber-security ecosystem shall be validated and evaluated against performance, effectiveness and usability indicators at three different countries (Romania, Portugal and Greece). Hospitals, healthcare providers and IT solution providers participating in the project's pilots will deploy and evaluate the solution at business-as-usual and emergency situations across various use case scenarios.

This report takes into account the SPHINX project characteristics and particularises them onto legal and ethical findings. Its first three parts elaborate upon the applicable legal and ethical framework for SPHINX project purposes. In this context, the ethical principles applicable are discussed in Chapter 1, while EU personal data protection law and EU cybersecurity law are analysed in Chapters 2 and 3 respectively. The analysis takes into account primary and secondary legislation, as well as, guidance issued by the European Commission and other EU bodies and agencies. Its aim is to formulate a comprehensive text of reference for all ethical and legal issues that are of relevance to the project.

Findings of the first three Chapters of this report are made concrete onto actual SPHINX circumstances in Chapter 4. While structurally the already applied pattern is followed in this Chapter as well (subchapters 4.3, 4.4 and 4.5 focusing on ethical, personal data protection, and cybersecurity issues respectively), attention has been given to drafting concrete and specific guidance to project partners in order to warrant compliance with the highest possible ethical and legal standards during project execution.

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.

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 Ethical principles applicable to research conducted in the EU

1.1 What are the major ethical issues in conducting research?

Respect of ethical principles and ethical compliance is an important requirement for all EU-funded projects. The Regulation establishing Horizon 2020[1] in its article 19, under the title "Ethical Principles", describes the main ethics' concerns and principles that should be taken into consideration when conducting research. In more detail, according to the Regulation, the ethical framework in Horizon 2020 is defined by five ethical principles:

a) All the research and innovation activities carried out under Horizon 2020 projects shall comply with ethical principles and relevant national, Union and international legislation, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its Supplementary Protocols. Particular attention shall be paid to the principle of proportionality, the right to privacy, the right to the protection of personal data, the right to the physical and mental integrity of a person, the right to non-discrimination and the need to ensure high levels of human health protection;

b) Research and innovation activities carried out under Horizon 2020 shall have an exclusive focus on civil applications;

c) In Horizon 2020 projects the following fields of research shall not be financed: research activity aiming at human cloning for reproductive purposes; research activity intended to modify the genetic heritage of human beings which could make such changes heritable; research activities intended to create human embryos solely for the purpose of research or for the purpose of stem cell procurement, including by means of somatic cell nuclear transfer;

d) Research on human stem cells, both adult and embryonic, may be financed, depending both on the contents of the scientific proposal and the legal framework of the Member States involved. No funding shall be granted for research activities that are prohibited in all the Member States. No activity shall be funded in a Member State where such activity is forbidden;

e) The fields of research set out in paragraph 3 of this Article may be reviewed within the context of the interim evaluation set out in Article 32(3) in the light of scientific advances[2].

Consequently, a list of the ethical issues that EU research projects ought to deal with includes:

- Informed consent;
- Civil application and dual use;
- Vulnerable subjects including patients, elderly and children;
- Privacy / confidentiality;
- Personal data;
- Potential misuse of research findings;
- Information security.

[1] Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC.

[2] Article 32(3) of the Regulation states that "By 31 December 2017, and taking into account the ex-post evaluation of the Seventh Framework Programme to be completed by 31 December 2015 and the review of the EIT, the Commission shall carry out, with the assistance of independent experts, selected on the basis of a transparent process, an interim evaluation of Horizon 2020, its specific programme, including the European Research Council (ERC), and the activities of the EIT [….]".

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.

1.2 The European Code of Conduct for research integrity

Ethical codes and guidelines are a useful tool in evaluating and establishing the values that any type of entity operating in an organised social environment should apply. At the same time, ethical codes, if applied correctly, may significantly contribute to the conduct of a correct self-assessment and ultimately of self-regulation of any matter (including ethical compliance) related to the organisation's function.

With regard to research in particular, the main tool used to this effect is the European Code of Conduct for Research Integrity[3]. The Code applies to research in all scientific and scholarly fields and has been recognised by the Commission as the reference document for research integrity for all EU-funded research projects, as well as a model for organisations and researchers across Europe.

The Code makes explicit reference to the fundamental principles of research integrity. Its list includes the following principles:

- Reliability in ensuring the quality of research, reflected in the design, the methodology, the analysis and the use of resources;
- Honesty in developing, undertaking, reviewing, reporting and communicating research in a transparent, fair, full and unbiased way;
- Respect for colleagues, research participants, society, ecosystems, cultural heritage and the environment;
- Accountability for the research from idea to publication, for its management and organisation, for training, supervision and mentoring, and for its wider impacts.

The aforementioned principles govern the internal process of conducting research and could be used as a guidance for researchers in their research work and in their collaboration with each other. They, therefore, warrant the integrity of the research and they should apply together with the ethical principles, as these shall be elaborated below under section 4.

1.3 Identifying and addressing ethical issues in research – the European Commission's "ethics issues table"

Identifying ethical issues and risks in research and suggesting measures to minimise or prevent them (and, of course, addressing them) is the key to safeguarding that research will indeed be conducted and completed in accordance with ethical principles and values. In order to help researchers to comply with such task the European Commission has issued guidelines on how to complete an ethics self-assessment[4]. Its document covers most of the issues arising in research projects and could provide some useful guidance on how to perform an ethics self- assessment.

The Commission's guidelines cover the following fields or categories of research:

- Research on human embryos and foetuses;
- Research on human beings;
- Research on human cells or tissues;
- Research which involves processing of personal data;
- Research involving animals;
- Research involving non-EU countries;

[3] http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf
[4] https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_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.

- Research that may adversely affect the environment, or the health and safety of the researchers involved;
- Research involving goods, software and technologies covered by the EU export Control regulation No 482/2009 (dual use items);
- Research that has an exclusive focus on civil applications;
- Research involving or generating materials, methods, technologies or knowledge that could be misused for unethical purposes.

For each category mentioned above the Commission's document provides an ethics issues checklist, as well as a list of information and documents that need to be provided together with the checklist. The ethics' issues table is considered up to date, however, any participant in research should be ready to identify and address any other ethical issues that are not covered by the Commission's guidance.

1.4 List of ethical issues

A list of the main ethical issues that may arise during the conduct of H2020-related research, as well as an indicative list of measures that could be undertaken in order to minimise and mitigate the infringement of ethical principles is discussed below.

1.4.1 Informed consent

A) Definition

Informed consent of the subjects participating in a research project is the first and arguably the most important part of conducting research ethically. It warrants that the subjects participate in the research voluntarily and at the same time it constitutes the safest procedure to address privacy issues in research. However, consent should meet specific conditions in order to be valid. In particular:

- It should be freely given;
- It should be obtained in advance;
- It should be in writing;
- It should be informed, based on adequate and accurate information;
- It should always be freely withdrawn.

The European textbook on ethics in research[5], published by the Commission, provides a tripartite definition of 'valid consent' according to which valid consent must include the following three elements:

- **Adequate information**
- **Voluntariness**
- **Competence**

Adequate information refers to both the quantity and the quality of information provided to the data subjects. Participants should be clearly informed of the research goals and possible adverse events. Voluntariness means in practice that the consent must not result from coercion, manipulation, or undue inducements. Finally, competence suggests that the person giving the consent has sufficient mental competence or capacity to understand and retain relevant information about the research, communicate his or her views on the research accordingly.

B) Official guidance on informed consent

[5] 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.

There is substantial official guidance that refers explicitly to respect for free and informed consent. For instance, **the Charter of Fundamental Rights of the EU[6],** in its, article 3 (Right to the integrity of the person) states that "*1. everyone has the right to respect for his or her physical and mental integrity. 2. In the fields of medicine and biology, the following must be respected in particular: the free and informed consent of the person concerned, according to the procedures laid down by law*". Article 5 of t**he Council of Europe's Convention for the Protection of Human Rights and Dignity with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine[7]** states that: "*An intervention in the health field may only be carried out after the person concerned has given free and informed consent to it. This person shall beforehand be given appropriate information as to the purpose and nature of the intervention as well as on its consequences and risks. 3 The person concerned may freely withdraw consent at any time"*.

The above are not meant to lead to the misconception that consent is required only in medical research. Informed consent is an ethical issue that should be addressed in all research fields where humans are involved. Individual consent as a condition for lawful processing of personal data as well as the ethical issues associated with such processing is elaborated below under 2.3.4.

c) List of information that should be provided to the subjects according to the Ethics for Researchers report by the Commission

The European Commission has published an ethics for researchers report[8] where it lists the information that should be provided to the research subjects before they participate in the research. This information includes:

- The purposes of the research and information about what will happen with the results of the research;
- The experimental procedures and a detailed description of the involvement of the participants, including the expected duration, and all the relevant procedures;
- All foreseeable risks or discomforts expected to occur for the research subjects during and after their participation;
- All benefits to the participants or to others which may reasonably be expected to occur;
- The insurance guarantees for the participants during and after participation and information on the foreseen treatments and compensations. Alternative procedures or treatments that might be advantageous to the participant need to be disclosed;
- Procedures in case of incidental findings;
- A description of the procedures adopted to guarantee the participant's privacy: the levels of confidentiality, the measures to protect the data, the duration of the storage of the data and what will happen with the data or samples at the end of the research;
- Contact details for researchers who can be contacted at any time to answer pertinent questions about the research and the participant's rights and that can be contacted in the event of a research related injury;
- A clear statement that the participation is voluntary, that the refusal to participate will involve no penalty or loss of benefits to which the participant would otherwise be entitled and that the participant may decide, at any time, to discontinue participation without penalty;
- Information about the organisation and funding of the research project.

d) Informed consent form and content

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN
[7] https://rm.coe.int/168007cf98
[8] http://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.

The European Commission in its document entitled "Horizon 2020 Programme Guidance How to complete your ethics self-assessment" provides some useful guidelines to participants in research on how to acquire a right and adequate informed consent from the research participants. In more detail:

1. Participants must be given an informed consent form and detailed information sheets that:

– are written in a language and in terms they can fully understand;

– describe the aims, methods and implications of the research, the nature of the participation and any benefits, risks or discomfort that might ensue;

– explicitly state that participation is voluntary and that anyone has the right to refuse to participate and to withdraw their participation, samples or data at any time without any consequences;

– state how biological samples and data will be collected, protected during the project and either destroyed or reused subsequently;

– state what procedures will be implemented in the event of unexpected or incidental findings (in particular, whether the participants have the right to know, or not to know, about any such findings).

2. Researchers must ensure that potential participants have fully understood the information and do not feel pressured or coerced into giving consent.

3. Participants must normally give their consent in writing (e.g. by signing the informed consent form and information sheets). If consent cannot be given in writing, for example because of illiteracy, non-written consent must be formally documented and independently witnessed.

4. Especially for the case of children or other persons unable to give consent, e.g. certain elderly populations, persons judged as lacking mental capacity the document suggests that researchers must obtain informed consent from the legally authorised representative and ensure that they have sufficient information to enable them to provide this on behalf and in the best interests of the participants. Whenever possible, the assent of the participants should be obtained in addition to the consent of the parents or legal representatives. Participants must be asked for consent if they reach the age of majority in the course of the personal data processing and/or research, as appropriate.

The Commission has also issued a guidance for applicants on informed consent (elaborated below, under 2.3.4).[9]

1.4.2 Civil application and dual use

a) Definitions

The notion of civil application should be examined together with that of dual use. European research funding is only possible for research with an exclusive focus on civil applications, excluding thus any military use. This is explicitly referred in Regulation No 1291/2013 establishing Horizon 2020[10]. In particular, article 19 of the Regulation, which addresses ethics, lists the ethical principles which all the research activities carried out under the Horizon 2020 should comply with, and, at the same time, limits the scope of the framework programme by excluding a number of research areas from funding. Article 19(2) states that: "Research and innovation activities carried out under Horizon 2020 shall have an exclusive focus on civil applications.

b) Application of the notions in research

[9] http://ec.europa.eu/research/participants/data/ref/fp7/89807/informed-consent_en.pdf
[10] See above footnote 1

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.

Dual use technologies and/or goods include technologies and goods that can address the needs of both civil and military users. Regulation 428/2009[11] defines in its article 2(1) dual use items as: "*items, including software and technology, which can be used for both civil and military purposes, and shall include all goods which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices".* Dual use technologies are not by default excluded from EU funding on the condition however that they are exclusively focused on civil applications. The Commission, in its Guidance note[12], clarifies that the actors involved in the research activity is not a factor that should be taken into consideration when assessing whether a research activity qualifies for funding. In particular, the fact that military partners or partners active in the defence industry or in military research participate in a project does not preclude the funding of the research. Additionally, the research topic should not affect the judgement of whether a research qualifies for funding either. In this context, the Commission's explanatory note mentions that projects involving the defence industry or military organisations are not automatically excluded from funding. Research on defence related subjects may still qualify for funding, as long as its aims are exclusively focused on civil applications.

Focus on civil application is an issue that should always be checked by all participants in research projects when conducting their ethics assessment.

1.4.3 Vulnerable subjects

a) Definition of vulnerability

Research on human subjects is thought to be ethically challenging particularly when human subjects belong to what we call "vulnerable groups". This section will focus on the issues that arise when research involves vulnerable groups of people. Which persons fall under this category, what are the challenges and what parameters should be taken into consideration and finally what special measures should be undertaken in order to safeguard their well-being are some of the questions that need to be answered when research focuses on vulnerable groups of people.

What needs to be answered first, in order to be able to present some further thoughts on the ethical issues arising from this type of research, is what vulnerability means. It seems that, so far, there is no single and commonly accepted definition of vulnerability. In this context, vulnerability is classified as one characteristic of people unable to protect their own rights and welfare. Another definition defines vulnerable groups 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 Organisations of Medical Sciences[13], 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.**

According to the Commission's European textbook[14] on ethics in research three main areas stand out as indications of subjects' vulnerability:

[11] Council Regulation setting up a Community regime for the control of exports, transfer, brokering and transit of dual use items

[12] https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-civil-apps_en.pdf

[13] https://cioms.ch/

[14] See above footnote 5

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.

- Subjects who lack competence will be unable to protect their interests by choosing to give or withhold consent;
- If the voluntariness of the subjects' consent is compromised, this may similarly prevent them from choosing to give or withhold consent in a way that would protect their interests;
- The physical (or psychological) condition of some subjects leaves them especially liable to harm, for example as a result of frailty through age, disability, or illness.

b) How could vulnerable groups be protected when participating in research

The general rule that should apply in all research projects involving vulnerable groups is that such involvement ought to be restricted to some extent. In other words, vulnerable groups should participate only when the specific research cannot be carried out with persons who are less vulnerable. Special justification for their involvement should always be provided. In the event that the above conditions are met and vulnerable groups indeed end up participating in research, there are some further actions that should be undertaken in order to better safeguard these subjects' rights. Some examples include:

- the research should be designed in such a way to respond to their needs or priorities;
- the research has benefits for the subject that override the disadvantages;
- improve the quality of consent by understanding what their incompetence consists of and how additional information could help them understand the scope and the purpose of the research;
- if acquiring consent is not an option, find alternatives to consent such as:
  a) gaining the subject assent; assent is not a substitute for consent, however it could be used as a means to respect the individual's autonomy to the extent he/she possesses it;
  b) use family or legally appointed representatives to make decisions on their behalf;
  c) rely on an advance statement that is a statement that has been prepared before the subject became incompetent;
  d) adopt measures to minimise the subjects' inconvenience;
  e) facilitate and simplify the opt-out process (vulnerable subjects should be able to leave the research at any time and without extra formalities).

1.4.4 Privacy / confidentiality

a) Definitions

Privacy and confidentiality are considered related issues in research ethics. Defining both terms is the first step in order to understand what the ethical implications of non-respecting or violating these principles would be.

The definition of **privacy** is not an easy and obvious one. The concept has appeared in many official documents through the years. For instance:

- The 1948 Universal Declaration of Human Rights[15], specifically protects territorial and communications privacy. Article 12 states: No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks.
- The European Convention on Human Rights[16] in its Article 8 states that: 1. Everybody has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or

[15] https://www.un.org/en/universal-declaration-human-rights/
[16] https://www.echr.coe.int/Documents/Convention_ENG.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 economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

- The Charter of Fundamental Rights of the EU[17] in its article 7 entitled respect for private and family life mentions that "Everyone has the right to respect for his or her private and family life, home and communications".

According to the Commission's "European Textbook on Ethics", privacy is the protection of:

- control over information about oneself;
- control over access to oneself, both physical and mental;
- control over one's ability to make important decisions about family in order to be self-expressive and to develop varied relationships.

Confidentiality on the other hand focuses on the aspect of privacy concerning the protection of personal information. Confidentiality is an obligation that arises when a person has acquired access to another person's information either by virtue of a contract or on the basis of a specific relationship (for instance lawyer-client relationship). Confidentiality in this sense is also related to trust. Keeping one's information safe confirms the disclosing person's correct decision in the first place to trust the recipient and share his/her valuable confidential information with him.

b) How should these principles apply in research?

It is evident that issues of privacy and confidentiality can arise in all forms of research involving human subjects and the gathering of information about them.

Privacy has to be respected when researchers acquire information about their subjects including their decision to take part in the research in the first place. Some of the measures that need to be undertaken by researchers when conducting their research are:

- acquire the research subject's informed consent. The importance of informed consent is examined above under 4.1. As already mentioned, informed consent is perhaps the most important step in warranting that the research will be conducted in an ethical manner. The subject needs to be informed about the research, its purpose, its potential outcome and any other parameters related to it;
- the subject needs to be always aware that he/she is part of a research;
- warrant that participation in research is the result of free will (special caution when vulnerable groups are involved);
- the subject should be free at all stages of the research to withdraw from the process;
- apply data protection mechanisms especially when sensitive data or vulnerable groups of people are involved;
- safeguard research subjects' dignity and autonomy throughout the process as a direct aspect of their privacy.

As far as **confidentiality** is concerned, this principle refers to how researchers may communicate the information they acquired from the research subjects. The main challenge for research is to use and share the data, and at the same time protect all identifiable information to guarantee personal privacy. Breach of confidentiality constitutes at the same time a breach of the person's privacy. The case where the researcher may be ethically required to breach the confidentiality obligation is an issue that exceeds the purpose of this analysis. We could however note that this could happen in practice when, for instance, the researcher is required to do so by law or when disclosing information will protect public interests (for instance public health).

[17] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

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.

In any event breach of confidentiality could be hindered by acquiring the subject's consent to disclose his/her confidential information or by anonymising the personal information and disclose it in an anonymised form.

1.4.5 Protection of personal data

a) Definition of personal data

According to the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and the of the Council)[18] and in particular its article 4 (1) "personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

b) The role of data protection in research

Data protection is a central issue when research ethics are being evaluated. Research subjects should, during all stages of research, be provided with detailed information regarding any parameter of processing of their personal data, for instance what kind of 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, is the data subject informed about their right to be forgotten etc. With regard to the kind of personal data in particular that may be used in research, these can include health information, genetic information, information on criminal records, financial information, information on religious beliefs and sexual orientation or ethnic identification.

The main ethic concern researchers should address when their research involves processing of personal data is how to safeguard the privacy of research subjects and how to protect their personal information. An even higher ethic risk is raised 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.

c) How to identify and address data protection issues in research

As with all ethical issues in research, data protection issues may also be addressed through the conduct of a data protection risk assessment. The assessment will help the researchers identify the special conditions, if any, that make processing of personal data during their research, of a high risk. At the same time, it will enable researchers to consider and ultimately implement the safest solutions in order to safeguard the personal data of people participating in their research. In any event all EU-funded research projects should comply with data protection legislation and more particularly with the General Data Protection Regulation. Compliance with the GDPR, including notions as informed consent, data minimisation, accountability, etc, as well as a list of the rights the data subjects may exercise (as these are described in the GDPR) are analytically examined below under Chapter 2.

1.4.6 Potential misuse of research findings

a) Definition – Research vulnerable to misuse

[18] https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-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.

A definition of misuse of research findings is included in the Commission's guidance note[19], as well as in the explanatory note[20] issued also by the Commission. On this basis, "potential misuse of research refers to research involving or generating materials, methods, technologies or knowledge that could be misused for unethical purposes".

According to the note the research most vulnerable to misuse is research that:

- provides knowledge, materials and technologies that could be channelled into crime or terrorism;
- could result in chemical, biological, radiological or nuclear weapons and the means for their delivery;
- involves developing surveillance technologies that could curtail human rights and civil liberties;
- involves minority or vulnerable groups or develops social, behavioural or genetic profiling technologies that could be misused to stigmatise, discriminate against, harass or intimidate people.

Misuse of research findings could be minimised if a sound risk assessment was performed. A detailed analysis on misuse of research findings including a special application to the SPHINX case in included deliverable D1.4.

1.4.7 Information security

a) Definition

Information security encompasses all measures taken to protect the information processed within a system (e.g. electronic, physical) from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Information security is represented by the so-called security triad (CIA triad) i.e., confidentiality, integrity, and availability of information. ENISA in its guidelines for SMEs on the security of personal data[21] processing has defined these three security principles as follows:

- **Confidentiality** is defined as the "property that information is not made available or disclosed to unauthorised individuals, entities, or processes". In practice, all the measures implemented to ensure confidentiality are designed to prevent the information from being accessed by unauthorized individuals, entities or processes, while ensuring that the authorised individuals, entities or processes have access to it.
- **Integrity** is defined as the property of "accuracy and completeness". In that sense, integrity implies maintaining the consistency, accuracy, and trustworthiness of information, over its entire life cycle. Data must not be changed in transit and measures must be undertaken to ensure that data cannot be altered by unauthorised individuals, entities or processes.
- **Availability** is defined as the property of "information being accessible and usable when an authorized party demands it". This means that the systems used to store and process information, as well as the information communication channels are all functioning correctly.

In practice this is best ensured by uncompromised maintenance of the hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is software conflicts free.

b) How to apply information security in research

Information security raises major ethical concerns especially in research activities. The reason for this is that valuable information could possibly be at stake that include both personal data- in many cases sensitive- and research findings. Safeguarding therefore the integrity, confidentiality and availability of such information

[19] https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-misuse_en.pdf
[20] https://ec.europa.eu/research/participants/portal/doc/call/h2020/fct-16-2015/1645168-explanatory_note_on_potential_misuse_of_research_en.pdf
[21] https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-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.

should always be a high priority for everyone involved in research. Insufficient information security could lead to breach of confidentiality and information integrity. The consequences of confidentiality violations as well research findings misuse could lead to serious complications and have been analysed above in the relevant sections.

Information security could be achieved through the adoption of adequate organisational and technical measures, as well as through the use of security policies. As in all other cases, best practice to address issues of information security is to conduct a sound information security risk management.

A risk management process comprises four (4) key phases:

- **Risk assessment**. The risk assessment starts with the identification of threats, followed by the determination of the relevant likelihood and the impact of each risk;
- **Risk treatment**: Based on the results of the risk assessment, at this phase the organisation selects and implements security measures to treat the risks;
- **Risk acceptance:** Even when the risks have been treated, residual risks will probably remain (e.g. due to the fact that some controls are not feasible). These risks will need to be accepted;
- **Risk communication**: All involved stakeholders need to be informed about risks adopted controls, as well as accepted risks.

Information security as a part of network and information systems shall be analytically examined under the NIS Directive section (under Chapter 3).

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 Personal Data Protection – Regulation EU 2016/679, its purpose and basic definitions

2.1 Background and purpose

The protection of natural persons in relation to processing of their personal data is a fundamental right protected under article 8(1) of the Charter of Fundamental rights of the European Union, as well as under article 16 (1) of the Treaty on the Functioning of the European Union.

Data protection in Europe was, until recently, regulated by the Data Protection Directive 95/46/EC. However, constant technological developments, digitalisation and globalisation, as well as people intension to share a huge amount of data online, have challenged the data protection regime and have called for a reform that will warrant a strong and coherent data protection framework in the EU. Effective protection of personal data throughout the Union, strengthening of the subjects' rights when processing of their personal data takes place, setting in detail data controllers' obligations and warranting free flow of personal data within the Union are only some of the issues the new General Data Protection Regulation (**GDPR**) aims to address.

The GDPR is the successor of Directive 95/46/EC of 24 October 1995. GDPR entered into force in May 2016 and became fully enforceable in May 2018 throughout the European Union. GDPR, contrary to the recently repealed Data Protection Directive, is a regulatory tool of catholic and direct effect that intends to address any inconsistency in national laws and to succeed a harmonised data approach among Member States.

GDPR regulates the processing by an individual, a company or an organization of personal data relating to individuals in the EU. The Regulation does not apply to the processing of personal data of deceased persons or of legal entities. Its provisions do not apply to data processing by an individual for purely personal reasons or for activities carried out in one's home provided there is no connection to a professional or commercial activity.

2.2 Definitions

The basic definitions under the GDPR, as of more relevance to the SPHINX project, include:

a) Personal Data

The definition of "personal data" is included in Article 4(1) of the GDPR: **personal data** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The notion of "identifiability" is further analysed in the Regulation and more specifically in Recital 26 where a proportionality test is used in order to assess each time what data may pertain to identifiable individuals. The recital reads as follows: "*To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments*". If the test is not passed, then such data are considered anonymous and the law does not apply on them.

b) Special categories of data

Special attention should be given to categories of data that do not fall under the generic definition of personal data mentioned above. These include

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.

- **genetic data** that include 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 include 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 refer to 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. The first two categories constitute additions in the data protection field that come as a result of scientific developments in their respective fields.

The above categories of data fall under the definition of special categories of personal data. It should be mentioned that the term sensitive data that was used in the Directive is replaced in the new Regulation by the term "special categories of personal data". According to article 9 (1) of the GDPR "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited". Exceptions to this rule are included in par. 2 of the same Article 9, as outlined below under (d).

c) Pseudonymisation

Another definition that should be included in this analysis as of relevance to the SPHINX project is that of "pseudonymisation". The term is a new entry in the text of the GDPR. In essence, pseudonymisation means "*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided such additional information is kept separately and subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable person*" (Art. 4(5)). For the avoidance of any doubt regarding whether or not pseudonymised data should be treated as personal data recital 26 of the GDPR clarifies that: "*personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person*". What matters in practice is not the process of pseudonymisation as such but whether the natural person could be, at the end of the day, be identified.

d) "Processing" of personal data

A definition of "processing" of personal data is provided under Article 4(2) of the Regulation. Processing therefore means "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*". The processing principles are described below under 2.3.

The Regulation makes explicit reference to processing of special categories of personal data in its article 9. In this context, apart from the basic principles that should apply to any processing of personal data, in the event that special categories of data are concerned, processing shall be prohibited. **Article 9(2) however names the exceptions to this general prohibition. In particular, paragraph 1 shall not apply if one of the following applies:**

a. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

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.

b. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
c. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
d. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
e. processing relates to personal data which are manifestly made public by the data subject;
f. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
g. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
h. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
i. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
j. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

e) Controllers – processors – joint controllers – recipients

The definition of a **controller** is provided under article 4(7) of the GDPR. According to said provision controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law". New addition introduced by the Regulation is the explicit reference to the notion of joint controllers. Article 26 of the Regulation states that "Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation […]".

Article 4(8) defines a **processor** as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

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, a **recipient** is defined under article 4(9). In particular, "recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not".

2.3 The GDPR processing principles

2.3.1 The personal data processing principles in general

Principles relating to processing of personal data are listed in Article 5 of the GDPR. If one wanted to compare the old legislative framework with the new one, one would reach the conclusion that the processing principles remain, in their essence, the same, however they have been worded in a more solid way. In addition, the principles of transparency and accountability have been added to the list of principles, thus contributing further to individual protection during processing of personal data.

In this context Article 5 of the Regulation reads as follows:

> 1. Personal data shall be:
>
> a. processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency'**)
>
> b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
>
> c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
>
> d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
>
> e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')
>
> f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').
>
> 2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

To sum up, the processing principles provided under the General Data Protection Regulation are the principles of:

- **lawfulness, fairness and transparency**
- **limited purpose**

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 minimisation**
- **accuracy**:
- **storage limitation**
- **integrity and confidentiality**
- **accountability**

2.3.2 Fair, lawful and transparent processing

a) Lawfulness

According to Article 5.1(a) of the EU GDPR, "*personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency)*". 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 and not cumulatively all six of them, needs to apply in order for the processing to be conducted lawfully.

Consequently, the lawful grounds for processing operations are six:

- **consent,**
- **performance of a contract,**
- **compliance with a legal obligation,**
- **protection of vital interests,**
- **public interest,**
- **overriding interest of the controller.**

b) Transparency

As far as **the principle of transparency** is concerned, article 5.1(a) of the GDPR states that personal data must also be processed in a transparent manner. Further guidance on what transparency exactly means is provided in Recital 39: *"[…] 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. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such*

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. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data.".

2.3.3 The principle of accountability

As already mentioned, the principle of accountability is a new addition under the GDPR. According to Article 5.2 of the EU 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 data controller's obligation to undertake the necessary measures, both organisational, technical or other in order to be ready, to demonstrate that the data protection law has been observed. Internal policies, appointment of a Data Protection Officer or conducting Data Protection Impact Assessments are some examples of compliance with the principle of accountability.

2.3.4 Individual consent

As indicated above under Chapter 1 (ethical principles), informed consent of the subjects participating in a research is the first and perhaps the most important part of conducting research ethically. When it comes to personal data processing in particular, individual consent is arguably the most important legal ground for processing personal data lawfully. It's the only legal ground that lies exclusively upon the individual's personal decision to have his/her personal data processed.

A definition of consent is provided under article 4(11) of the GDPR: consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

More details on the specific criteria which individual consent should meet are provided under recital 32 of the GDPR: "*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 or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. 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. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided*".

Additional conditions for consent are listed in article 7 of the Regulation. In more detail:

- the controller shall be responsible to demonstrate that the data subject has consented to processing of his or her personal data;
- if consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters;
- the data subject shall be free to withdraw his/her consent at any time;
- When the performance of a contract is conditional on consent to the processing of personal data that is not necessary for the performance of that contract, it should always be examined whether the consent has indeed be provided freely;

The Regulation refers separately to the conditions applicable to child's consent in relation to information society services (Article 8 of the GDPR).

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.

It is noted that the notion of consent and all matters related to it as far as personal data processing is concerned shall be examined in detail under Deliverable D1.10.

2.4 The GDPR rights afforded to individuals (data subjects)

2.4.1 General

Rights of the data subject are dealt with in Chapter III of the GDPR. In particular, Article 12 sets the way (the "modalities") that rights listed in the next articles are to be exercised:

- any information to the data subjects should be provided by the controller in a transparent and easily accessible form;
- the information shall be provided in writing;
- the controller shall facilitate the exercise of the data subjects' rights;
- the controller shall also provide information on action taken on a request under Articles 15-22 to the data subject without undue delay;
- if the controller does not take action on the request of the data subject, the controller shall inform the data subject of the reasons for not taking action;
- information shall be provided for free.

The rights attributed to data subjects are regulated under articles 13 to 21 and are the right to information, the right of access, the right to rectification, the right to erasure (right to be forgotten), the right to restriction of processing, the right to data portability, and the right to object.

2.4.2 The right to information

The right to information 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. In this case, the controller shall at the time when personal data are obtained, provide the data subject with the following information:

a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

b) the contact details of the data protection officer, where applicable;

c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

e) the recipients or categories of recipients of the personal data, if any;

f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

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.

Paragraph 2 of Article 13 lists the additional information the controller needs to provide to the data subject when collecting his/her personal data, such as 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 time etc.

Article 14 lists the information to be provided to the data subject where personal data have not been obtained from the data subject itself. Paragraph 5 of article 14 sets some exemptions of the controllers' obligation to provide information, for instance when the provision of such information proves impossible or would involve a disproportionate effort or where personal data must remain confidential etc.

2.4.3 The right to access the data

The right of access by the data subject is regulated under article 15 of the Regulation. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him/her are being processed and if yes, access to such data as well as information regarding, among others, the purpose of processing, the recipients to whom the data have been or will be disclosed the existence of the right to request rectification, the right to lodge a complaint and others, the right to request rectification etc. Paragraph 3 of article 15 sets the subject's right to request a copy of his/her personal data from the controller.

It is noted that the right to rectification is regulated separately in article 16. In particular, the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.

2.4.4 The right to erasure (right to be forgotten)

Article 17 of the Regulation grants individuals the right to have their personal information deleted by data controllers if specific conditions as these are listed in its paragraph 1 are met. For instance, the personal data have been unlawfully processed or they are no longer necessary in relation to the purpose for which they were collected, or the data subject has withdrawn his/her consent and others. In the event that the controller has made such data public, reasonable steps (including technical measures) will be taken to notify controllers who are processing the personal data accordingly. Finally, the "right to be forgotten" (actually, to erasure of data) will not be applicable if it contrasts with the rights of freedom of expression and information as well as for several other, more expected, legal grounds (compliance with a legal obligation, public interest, archiving purposes, etc., as set in paragraph 3).

2.4.5 The right to restriction of the processing

Article 18 of the Regulation regulates the right to restriction of the personal data processing. The conditions under which a data subject may exercise his/her rights are listed in the first paragraph of article 18 and include, for instance, the contest by the data subject of the accuracy of the personal data processed by the controller or the claim that the processing is unlawful and therefore the data subject opposes the erasure of his/her personal data. Recital 67 mentions some methods the controller may use to restrict the processing of personal data, such as, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website.

2.4.6 The right to data portability

Data portability is dealt with under article 20 of the GDPR and includes the data subject's right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. The right to data portability is provided to data subjects under two conditions:

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. the processing is carried out by automated means;

b. the processing is based on consent or on a contract.

2.4.7 The right to object

The right to object is laid down in Article 21 of the GDPR. Recital 69 of the Regulation clarifies the conditions under which a data subject may object to his/her data being processed. The recital reads as follows: Where personal data might lawfully be processed because 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, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject. In other words, the exercise by an individual of its right to object to its personal data being processed by a controller essentially includes a balancing of rights and legitimate interests: on the one hand an individual is interested in having its data no longer processed and on the other hand a controller may have an interest in continuing to process such data despite the individuals' objections.

2.5 Security of personal data

2.5.1 Security of the personal data processing

Security of the processing is regulated under article 32 of the GDPR. Both the controller and the processor need to implement technical and organisational measures to ensure a level of security including among others:

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 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 processing.

All measures should be proportionate to the risk involved and the severity for the rights and freedoms of natural persons in the event of a personal data breach.

2.5.2 Data Breach Notifications

Articles 32 and 33 regulate the process of notifying to the supervisory authority a personal data breach. A "personal data breach" is defined in the text of the GDPR, in Article 4(12), as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed*". When this happens, controllers shall, according to article 33, par. 1 "*without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay*". The obligation of notification burdens the processor as well, who, shall notify the controller without undue delay after becoming aware of a personal data breach (article 33 par.2). Paragraph 3 lists the minimum information the notification must contain, such as the nature of the data breach, the name and contact details 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.

protection officer, the likely consequences of the personal data breach and the measures taken or proposed to be taken by the controller to address the personal data breach.

Whereas article 33 deals with the notification of a breach to the supervisory authority, article 34 regulates the communication of a data breach to the data subject. This obligation burdens the controller in any case where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in article 33(2). Paragraph 3 of article 34 sets the conditions under which the communication to the data subject is not required. In particular par. 3 reads as follows "*The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner".*

2.6 Data protection impact assessment

The "tool" of the impact assessment is a new entry under the GDPR. It is suggested as an extra security measure in all cases where a type of processing is likely to result in high risk to the rights and freedoms of natural persons. The assessment of the impact of the envisaged processing operations on the protection of personal data is carried out by the processor prior to the processing. Par. 3 of the article 35 specifically lists the case where a data protection impact assessment shall be required:

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.

Paragraph 7 of article 35 lists the minimum content of the assessment. In particular, it should contain:

- a description of the processing and its purposes;
- an assessment of the necessity and proportionality of the processing in relation to the purpose of the processing;
- an assessment of the risks to the rights and freedoms of data subjects;
- the measures envisaged to address the risks, including security measures and mechanisms, to ensure the protection of personal data and to demonstrate compliance with the GDPR.

2.7 The case of SMEs

Special reference is made under the GDPR as far as micro, small and medium-sized enterprises are concerned. More specifically Recital 13 states that "*a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium -sized enterprises. To take account of the specific nature for micro, small and medium-sized enterprises, this regulation includes a derogation for organisations with fewer than 250 employees with regard to record keeping*." The special treatment of SMEs under the GDPR is also apparent in Recital 167 which mentions that the Commission should consider specific measures for micro, small and medium-sized enterprises. The specific needs of micro, small and medium-sized enterprises

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.

should also be taken into account when drawing up codes of conduct according to article 40 of the Regulation. This is also the case when establishing data protection certification mechanisms (article 42).

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 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures of a high common level of security of network and information systems across the Union (the NIS Directive)

3.1 The NIS Directive's purpose and scope

Directive 2016/1148 on security of network and information systems (the NIS Directive)[22] is the first horizontal legislation undertaken at European Union (EU) level for the protection of network and information systems across the Union. This legislative tool aims at addressing the constantly increasing threats, as well as deliberate actions that intend to cause disruption to IT services and critical infrastructures. Therefore, the security of network and security systems is a high priority across the EU and as such it needs to be addressed in a common way by all Member States. This need is evident in the Directive's text where in its first article it is stated that: "*The Directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market".*

The NIS Directive was published in July 2016, however the EU has been addressing cyber security issues in a comprehensive manner since 2004, when ENISA (European Union Agency for Network and Information Security), a new specialised EU agency, was founded. The NIS Directive itself has its roots in the Commission's Communication of 2009, which focuses on prevention and awareness and defines a plan of immediate action to strengthen the security and trust in the information society. This was followed, in 2013, by a joint Communication released by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy on the Cybersecurity Strategy of the European Union. From 2013 to 2015 the Commission, the Council and the Parliament discussed the draft put forward by the Commission intensely and these discussions resulted in the NIS Directive, that entered into force in August 2016. The deadline for national transposition by the EU Member States was the 9th of May 2018.

3.2 Basic definitions

Some of the main definitions included in the NIS Directive's text, as of relevance to the SPHINX project, may be seen below:

- **network and information system** mean:

  (a) an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC (transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;

  (b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or

[22] https://eur-lex.europa.eu/eli/dir/2016/1148/oj

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.

(c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance.

- **security of network and information systems** means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;
- **digital service** means a service within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (service' means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services). For the purposes of this definition:

  (i) "**at a distance**" means that the service is provided without the parties being simultaneously present;

  (ii**) "by electronic means**" means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;

  (iii) "**at the individual request of a recipient of services**" means that the service is provided through the transmission of data on individual request.

- **digital service provider** means any legal person that provides a digital service.
- **operator of essential services** means a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2), that is:

  (a) an entity that provides a service which is essential for the maintenance of critical societal and/or economic activities;

  (b) the provision of that service depends on network and information systems; and

  (c) an incident would have significant disruptive effects on the provision of that service.

- **incident** means any event having an actual adverse effect on the security of NIS.

3.3 The NIS Directive's application to operators of essential services and digital service providers

3.3.1 General

The NIS Directive applies to both operators of essential services and digital services providers. Their definitions are included in articles 4 and 5 of the Directive but should be examined in combination with the Directive's annexes, as well as Directive EU 2015/1535[23]. It should be mentioned that undertakings providing public communication networks or publicly available communications services[24], and trust services providers[25], as well as the sectors of banking and financial markets are excluded from the scope of the NIS Directive.

[23] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L1535

[24] Framework Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services

[25] Regulation 910/2014 on electronic identification and trust services for electronic transactions in the Internal market and repealing Directive 1999/93/EC

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.

3.3.2 Operators of essential services

It is noted that this analysis focuses on digital services providers and not operators of essential services. The reason for that is that the SPHINX project focuses on the provision of digital services (a cybersecurity tool) and does not therefore fall under the definition of an operator of essential services. However, for consistency reasons, a short presentation of the definition attributed to operators of essential services in the context of the NIS Directive has been included. **The term operator of essential services** includes a public or private entity that activates in specific sectors such as the sector of energy, health, transport and any other sector of the ones listed of a type referred in Annex II of the NIS Directive.

Article 5 of the NIS Directive specifies the criteria for the identification of the operators of essential services. For an entity to be characterised as "operator of essential services", the following criteria should be met:

(a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;

(b) the provision of that service depends on network and information systems; and

(c) an incident would have significant disruptive effects on the provision of that service. The definition of "significant disruptive effect" is given under Article 6 of the Directive.

Article 5 states that all Member States shall, by 9 November 2018, for each sector and subsector of referred to in the Annex, identify the operators of essential services with an establishment on their territory. Such list will be updated by the Member States ate least every two years after 9 May 2018.

Consequently, not all operators of essential services fall within the scope of the NIS Directive. Member States are tasked with the process of their categorisation and identification in order to determine which individual companies meet the criteria of the definition of operators of essential services.

3.3.3 Digital Service Providers – the online marketplace in particular

a. Definition of digital service providers

The NIS Directive applies also to digital services providers. The reason behind the decision of their inclusion in the Directive's scope is given in Recital 48 of the NIS Directive which reads as follows: "*Many businesses in the Union rely on digital service providers for the provision of their services. As some digital services could be an important resource for their users, including operators of essential services, and as such users might not always have alternatives available, this Directive should also apply to providers of such services*".

The definition of digital service provider is given under Article 4(6), and includes any legal person that provides a digital service. Digital service means a service within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 which is of a type listed in Annex III of the NIS Directive, namely **online marketplace**, **online search engine** and **cloud computing service**. These three types of services were chosen to be regulated due to the increasing number of businesses that fundamentally rely on them for the provision of their own services.

b. Definition of an online marketplace

As it will thoroughly be examined below under section 4.5 the SPHINX project itself doesn't fall under the definition of a digital service provider. However, the project will lay the necessary groundwork enabling its future development to actually offer digital services and in particular services that could attribute to SPHINX the definition of an online marketplace. The exact details on its possible categorization as such will be provided in section 4.5 of this report. For the purposes of this section, a definition of online marketplace is provided. The NIS Directive defines **"online marketplace"** as a digital service that allows consumers and/or traders (as

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.

respectively defined in points (a) and (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council[26] to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace.

According to points (a) and (b) of Article 4(1) of Directive 2013/11/EU,

(a) "**Consumer**" means any natural person who is acting for purposes which are outside his trade, business, craft or profession;

(b) "**Trader"** means any natural persons, or any legal person irrespective of whether privately or publicly owned, who is acting, including through any person acting in his name or on his behalf, for purposes relating to his trade, business, craft or profession;

Recital 15 of the NIS Directive gives **an additional definition for an online marketplace** which could prove very useful when defining the boundaries of the Directive's implementation on the SPHINX project. "*An online marketplace allows consumers and traders to conclude online sales or service contracts with traders and is the final destination for the conclusion of those contracts. It should not cover online services that serve only as an intermediary to third-party services through which a contract can ultimately be concluded. It should therefore not cover online services that compare the price of particular products or services from different traders, and then redirect the user to the preferred trader to purchase the product"*. **Application stores, which operate as online stores enabling the digital distribution of applications or software programs from third parties, are to be understood as being a type of online marketplace.**

Finally, ENISA has contributed to further clarifying what a marketplace is by stating in its guidelines released in February 2017[27] that "*There are no special provisions as to what can be sold through online market places, so it applies to all types of contracts (products and services). Although from a technical perspective most online marketplaces use an Incident notification for DSPs in the context of the NIS Directive website or web related technologies for delivering their services, it should not be a restriction in this sense, as mobile application stores make use of other technologies also"*.

3.4 Security and notification requirements for Digital Service Providers

3.4.1 How are digital service providers treated in the context of the NIS Directive

The NIS Directive provides a lighter regime for digital service providers compared to operators of essential services. The softer approach towards digital service providers is mainly based on the different nature of the infrastructures they use as well as of the services they provide. In this context, recital 57 of the Directive states that "*Given the fundamental differences between operators of essential services, in particular their direct link with physical infrastructure, and digital service providers, in particular their cross-border nature, this Directive should take a differentiated approach with respect to the level of harmonisation in relation to those two groups of entities. For operators of essential services, Member States should be able to identify the relevant operators and impose stricter requirements than those laid down in this Directive. Member States should not identify digital service providers, as this Directive should apply to all digital service providers within its scope*". In addition, recital 49 of the NIS Directive mentions that " […] *the security requirements for digital service providers*

[26] on attacks against information systems and replacing Council framework Decision 2005/222/JHA
[27] https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers

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.

should be lighter. Digital service providers should remain free to take measures they consider appropriate to manage the risks posed to the security of their network and information systems".

3.4.2 Security requirements for digital service providers under article 16 of the NIS Directive

The NIS Directive describes, in its article 16, the security measures that digital service providers should take in order to mitigate the risks that threaten the security of the network and information systems they use for the provision of their service. The same article regulates the incident notification process digital service providers should follow in order to comply with the provisions of the Directive.

Article 16 (1) lists the elements that need to be taken into account by Member States when they consider what measures they should adopt in order to manage the risks posed to the security of their network and information systems. These are:

a. The security of the systems and facilities;

b. Incident handling;

c. Business continuity management;

d. Monitoring, auditing and testing;

e. Compliance with international standards.

It is noted that the Commission, by virtue of article 16(8) of the NIS Directive,[28] issued an Implementing Regulation[29] that specifies further these elements, as well as the parameters to be taken into account in order to determine whether an incident has a substantial impact on the provision of those services.

According to the Implementing Regulation the elements of article 16 (1) are further described as follows:

a) Security of systems and facilities shall include the following elements:

- the systematic management of network and information systems, which means a mapping of information systems and the establishment of a set of appropriate policies on managing information security, including risk analysis, human resources, security of operations, security architecture, secure data and system life cycle management and where applicable, encryption and its management;
- physical and environmental security, which means the availability of a set of measures to protect the security of digital service providers' network and information systems from damage using an all-hazards risk-based approach, addressing for instance system failure, human error, malicious action or natural phenomena;
- the security of supplies, which means the establishment and maintenance of appropriate policies in order to ensure the accessibility and where applicable the traceability of critical supplies used in the provision of the services;
- the access controls to network and information systems, which means the availability of a set of measures to ensure that the physical and logical access to network and information systems, including

[28] The Commission shall adopt implementing acts in order to specify further the elements referred to in paragraph 1 and the parameters listed in paragraph 4 of this article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in article 22(2) by 9 August 2017.

[29] Commission Implementing Regulation (EU) 2018/151, of 30 January 2018, laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

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.

administrative security of network and information systems, is authorized and restricted based on business and security requirements.

b) Incident handling: measures to be taken by the digital service provider

- detection processes and procedures maintained and tested to ensure timely and adequate awareness of anomalous events;
- processes and policies on reporting information security incidents and identified weaknesses and vulnerabilities in their information systems;
- a response in accordance with documented procedures and reporting the results of the measure taken;
- an assessment of the incident's severity, documenting knowledge from incident analysis and collection of relevant information which may serve as evidence and support a continuous improvement process.

c) Business continuity management shall include:

- the establishment and the use of contingency plans based on a business impact analysis for ensuring the continuity of the services provided by digital service providers which shall be assessed and tested on a regular basis for example, through exercises;
- disaster recovery capabilities which shall be assessed and tested on a regular basis for example, through exercises.

d) The monitoring, auditing, and testing shall include the establishment and maintenance of policies on:

- the conducting of a planned sequence of observations or measurements to assess whether network and information systems are operating as intended;
- inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, and efficiency and effectiveness targets are being met;
- a process intended to reveal flaws in the security mechanisms of a network and information system that protect data and maintain functionality as intended. Such process shall include technical processes and personnel involved in the operation flow.

e) Compliance with international standards means standards that are adopted by an international standardization body as referred to in point (a) of Article 2(1) of Regulation (EU) No 1025/2012. Pursuant to Article 19 of Directive (EU) 2016/1148, European or internationally accepted standards and specifications relevant to the security of network and information systems, including existing national standards, may also be used.

3.4.3 Notification requirements for digital service providers under Article 16 of the NIS Directive

a) General

Except for the security requirements mentioned above, in order for a digital service provider to safeguard the security of its network and information system, an incident notification procedure should be followed. The obligation of DSPs to notify any incidents with a substantial impact on the provision of their service is regulated under Article 16 par 3 and 4 of the Directive. In particular, digital service providers shall **take measures to prevent and minimise the impact of incidents affecting the security of their systems and at the same time notify the competent authority or the CSIRT of any incident with a substantial impact on the provision of their service**.

It is pointed out that, according to article 16 (4), digital service providers are burdened with the obligation to notify an incident only in those cases where they have access to the information needed to assess the impact of an incident. As with security requirements, notification requirements for digital service providers are also

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.

lighter. ENISA comments on this lighter approach towards DSPs in its 2017 incident notifications for DSPs in the context of the NIS Directive paper where it states that "*In this respect, the light-touch approach aims at avoiding overburdening the DSPs while not hampering the capacity of the EU to react to cybersecurity incidents in a swift and efficient manner. Therefore, there are reasons to be concerned that a significant lowering in the requirements of incident notification (types of incidents, parameters to be used) could result in hindering the capacity (at EU or national level) to follow up on specific incidents threatening the functioning of the internal market at various levels*".

b) Substantial impact

The obligation of digital service providers to notify an incident is limited to incidents having a substantial impact on the provision of their services. In other words, not all incidents need to be notified to the competent authorities. According to par. 4 of article 16, the impact of an incident is substantial based on the following criteria:

(a) the number of users affected by the incident, in particular users relying on the service for the provision of their own services;

(b) the duration of the incident;

(c) the geographical spread with regard to the area affected by the incident;

(d) the extent of the disruption of the functioning of the service;

(e) the extent of the impact on economic and societal activities.

c) Substantial impact according to the Implementing Regulation

According to the Implementing Regulation (article 4), an incident shall be considered as having a substantial impact where at least one of the following situations has taken place:

- the service provided by a digital service provider was unavailable for more than 5 000 000 user-hours whereby the term user-hour refers to the number of affected users in the Union for a duration of 60 minutes;
- the incident has resulted in a loss of integrity, authenticity, or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via a network and information system of the digital service provider affecting more than 100.000 users in the Union;
- the incident has created a risk to public safety, public security or of loss of life;
- the incident has caused material damage to at least one user in the Union where the damage caused to that user exceeds EUR 1 000 000.

The Implementing Regulation lists also in its article 3 the parameters that determine the substantial impact of an incident. In particular and with regard to each criterion of article 16 (4) of the NIS Directive, the following should be taken into consideration:

Number of users: the digital service provider shall be in a position to estimate either of the following:

- the number of affected natural and legal persons with whom a contract for the provision of the service has been concluded; or
- the number of affected users having used the service based in particular on previous traffic data.

The duration of an incident, meaning the time period from the disruption of the proper provision of the service in terms of availability, authenticity, integrity or confidentiality until the time of recovery.

The geographical spread with regard to the area affected by the incident: the digital service provider shall be in a position to identify whether the incident affects the provision of its services in specific Member States.

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 extent of disruption of the functioning of the service: this shall be measured as regards one or more of the following characteristics impaired by an incident: the availability, authenticity, integrity or confidentiality of data or related services.

The extent of the impact on economic and societal activities: the digital service provider shall be able to conclude, based on indications such as the nature of his contractual relations with the customer or, where appropriate, the potential number of affected users, whether the incident has caused significant material or non-material losses for the users such as in relation to health, safety, or damage to property.

d) Substantial impact according to ENISA's guidelines

The notion of substantial impact is also examined under ENISA's guidelines[30]. To this end ENISA provides a further elaboration of the parameters that must be taken into account when determining the impact of an incident, as these are provided under article 16 (4) of the NIS Directive. In more detail:

- **Number of users affected by the incident.** ENISA's analysis is led by the methodologies used by DSPs when assessing the number of the users affected. In this context the following measurement units were identified: corporate subscribers, non-subscribers (visitors), reliant services and individual subscribers/accounts. DSPs have visibility only at the first layer of users, namely the ones that have directly accessed the initial services and are considered users by the initial DSP.
- **Duration of the incident.** ENISA's report provides for a definition of duration of an incident as following "*NIS downtime= the period of time when a digital service provided by a DSP is unavailable or unsecured (confidentiality, integrity or authenticity affected)*".
- **Geographical spread.** According to ENISA's guidelines, the term geographical spread as referred to in the NIS Directive could be defined as follows: "*Member States or regions within the EU where users were affected by impairments (NIS downtime) of the digital service provided by the DSP*". The report points out that this parameter is difficult to be evaluated. In practice f*or a DSP that offers online web access to its services, the identification of the exact countries or geographical areas affected might be impossible without the use of estimations based on previous data*.
- **Extent of the disruption of the functioning of the service. E**xtent of the disruption should be evaluated by taking into account the availability factor, as well as confidentiality, integrity and authenticity. The report concludes to the following definition of "extent of disruption": *extent of the disruption of the functioning of the service= the number of protection goals affected due to an incident disturbing a digital service offered by a DSP"*.
- **Extent of the impact on economic and societal activities.** This parameter is the least utilised by the industry. The report defines impact on economic and societal activities as follows "*by impact on economic and societal activities reference is made to possible damages brought to the functioning of the EU internal market, meaning the encompassing markets in the EU's 28 member states*". The extent of the impact on economic and societal activities is consequently defined as: "*the effects produced by a cybersecurity incident at DSP level that, as a result, affected the overall community, disrupting its normal functioning, generating either economic or social negative consequences*".
- **Other issues related to parameters.** The guidelines raise also the issue of the lack of distinction between the three types of DSPs in the Directive's text. In this context it is pointed out that there should be a distinction given the different factors that differentiate the providers of digital services, such as technical particularities, criticality etc. It is on this basis that cloud services are considered the most critical out of the three, the online market places follow and when it comes to search engines, the

[30] https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive

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.

situation is considered even less critical (in the sense that one can always turn to another provider in case of failure of one's favorite engine).

In view of the above, the NISD does not restrict the adoption of subsequent policies that distinguish between the types of DSPs. However, it is pointed out in this report that the technical particularities for each of the three types of DSPs should be addressed early on, since not addressing them might eventually prove to be a mistake (as already mentioned some parameters required by the NIS Directive cannot be measured in the same way for the different providers).

3.5 National Strategies and national authorities on the security of network and information systems

3.5.1 General

Each Member State must adopt a national framework in order to succeed compliance with the provisions of the NIS Directive. The national framework includes the national strategy on the security of network and information systems and the designation of the authorities that shall be responsible for the monitoring the implementation of the NIS Directive. According to article 7 of the NIS Directive, this national strategy shall address a list of issues such as a risk assessment plan, a governance framework to achieve the objectives of the national strategy, the objectives and priorities of the national strategy on the security of network and information systems etc.). Member States are obligated to communicate their national strategies to the Commission within three months from their adoption (article 7 (3)).

The authorities and other bodies that shall be tasked with the role of monitoring application of the NIS Directive at national and EU level are specified in articles 8, 9, 11 and 12 of the Directive.

3.5.2 National authorities

The Directive sets the obligation of Member States to designate one or more national competent authorities on the security of network and information systems, as well as a national single point of contact to the same effect (article 8). The competent authorities shall monitor the application of the Directive at national level. The competent authorities and single point of contact shall, whenever appropriate and in accordance with national law, consult and cooperate with the relevant national law enforcement authorities and national data protection authorities.

Each Member State shall notify to the Commission, without delay, the designation of the competent authority and single point of contact, their tasks, and any subsequent change thereto. The Commission shall publish the list of designated single points of contacts.

Additionally, to the designation of the competent authority and the single point of contact each Member State shall designate one or more computer security incident response teams CSIRTs (Article 9). A CSIRT may be established within a competent authority. Their requirements and tasks are described in Annex 1 of the Directive. The CSIRTs role, as per Annex I of the Directive, is to monitor incidents at national level, provide early warning, alerts and information to relevant stakeholders about risks and incidents, respond to incidents, provide dynamic risk and incident analysis and increase situational awareness, as well as, to participate in a network of the CSIRTs across Europe.

3.5.3 The Cooperation Group and the CSIRTs Network

As far as cooperation at EU level is concerned, a Cooperation Group is established under the Directive (Article 11). The Cooperation Group shall be composed of representatives of the Member States, the Commission and ENISA (European Union Agency for Network and Information Security). Its tasks are described in Article 11 par.

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 (it shall provide strategic guidance for the activities of the CSIRT network, exchange best practice between Member States, as well as information on research and developing relating to security of network and information systems etc.). The Group's functioning is further clarified by the Implementing Decision issued by the Commission, by virtue of article 11(5) of the Directive.

Finally, Article 12 establishes the creation of a network of the national CSIRT's. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT-EU. Among the tasks that fall within the CSIRTs Network's competencies are: exchange information on CSIRTs' services, operations and cooperation capabilities, exchange and discussing information related to incidents and associated risks (on request, on a voluntary basis), identify a coordinated response to an incident (on request), providing MS support in addressing cross–border incidents (on a voluntary basis) etc.

3.6 ENISA: The EU Agency for Cybersecurity

3.6.1 General

ENISA is the European Union Agency for Cybersecurity. It is located in Greece (Heraclion, Crete) and it has an operational office in Athens. ENISA was founded by Regulation (EC) No 460/2004 whereas its current regulatory framework consists of Regulation (EU) No 2019/881 of the European Parliament and of the Council (the EU Cybersecurity Act), that only recently came into effect (on 27 June 2019).

ENISA was set up in 2004 and since then is actively contributing to a high level of network and information security (NIS) within the Union. ENISA's mandate is to achieve "a high common level of cybersecurity across the Union" (Article 3.1 of the EU Cybersecurity Act). In particular it shall do so by being a "center of expertise", and also by acting as a reference point for advice and expertise on cybersecurity for EU stakeholders (Articles 4.1 and 3.1 of the EU Cybersecurity Act respectively).

3.6.2 ENISA's contribution to Network and Information Security

ENISA's contribution to network and information security includes:

- Issuing Recommendations;
- Carrying out activities that support policy making and implementation;
- "Hands-On" work, whereby ENISA collaborates directly with operational teams throughout the EU.

A summary of ENISA's strategy for the years 2016-2020 is being published and can be reached at https://www.enisa.europa.eu/publications/corporate/enisa-strategy. The strategy incorporates the following priorities:

a. Anticipate and support Europe in facing emerging network and information security challenges.

b. Promote network and information security as an EU policy priority.

c. Support Europe in maintaining state of the art NIS capacities.

d. Foster the emerging European NIS Community

e. Reinforce ENISA's impact

3.6.3 ENISA's contribution to implementation of the NIS Directive

ENISA's role in implementing the provisions of the NIS Directive is embedded in its text. More particularly, Recital 36 of the NIS Directive states that "ENISA should assist the Member States and the Commission by providing expertise and advice and by facilitating the exchange of best practice. In particular, in the application of this Directive, the Commission should, and Member States should be able to, consult ENISA." Recital 38

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.

states that "*In general, ENISA should assist the Cooperation Group in the execution of its tasks, in line with the objective of ENISA set out in Regulation (EU) No 526/2013 of the European Parliament and the Council (1), namely to assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information system security under existing and future legal acts of the Union. In particular, ENISA should provide assistance in those areas that correspond to its own tasks, as set out in Regulation (EU) No 526/2013, namely analysing network and information system security strategies, supporting the organisation and running of Union exercises relating to the security of network and information systems, and exchanging information and best practice on awareness-raising and training. ENISA should also be involved in the development of guidelines for sector-specific criteria for determining the significance of the impact of an incident*". Finally, Recital 69 states that "*When adopting implementing acts on the security requirements for digital service providers, the Commission should take the utmost account of the opinion of ENISA*".

In practice and with regard to digital service providers, ENISA has issued a report concerning the minimum security measures for digital service providers[31], as well as another set of guidelines to further describe the incident notification process imposed on DSPs as per article 16 of the NIS Directive[32].

The objectives of the report on the security requirements are summarised to the following:

- Define common baseline security objectives for Digital Service Providers (DSPs);
- Describe different levels of sophistication in the implementation of security objectives;
- Map the security objectives against well-known industry standards, national frameworks and certification schemes.

With regard to the guidelines on the incident notification, they significantly contribute to further elaborating and clarifying notions that are included in the Directive's text, such as the "incidents" that fall within the notification obligation, the term "substantial impact" as well as the "parameters" that must be taken into account when determining the impact of an incident, as these are included in article 16 (4) of the NIS Directive.

With regard to incident the guidelines adopt the following definition "Any incident affecting the availability, authenticity, integrity or confidentiality of data stored, transmitted or processed by a digital service provider (DSP) through network and information systems, which has a substantial impact on the provision of the digital service offered". The definitions of substantial impact and parameters are analysed above under 3.4.3.

[31] https://www.ENISA.europa.eu/publications/minimum-security-measures-for-digital-service-providers

[32] https://www.ENISA.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive

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 The SPHINX case: Ethical, legal and cybersecurity requirements applicable to the SPHINX project

4.1 Project's description

SPHINX aims to introduce a universal cyber security toolkit that will enhance the cyber protection of Health IT Ecosystem and ensure the patients data privacy and integrity. The SHPINX toolkit will be easily adapted or embedded on existing, medical, clinical or health available infrastructures. In the context of the project, SPHINX's cyber-security ecosystem shall be validated and evaluated against performance, effectiveness and usability indicators at three different countries (Romania, Portugal and Greece). Hospitals, health care providers and IT solution providers participating in the project's pilots will deploy and evaluate the solution at business as usual and emergency situations across various use case scenarios.

4.2 Project's particularities

All EU-funded projects need to comply with ethical principles, as well as with any applicable international, EU and national law. To this effect, it should be made certain that the SPHINX project meets the relevant compliance standards. This analysis aims to address any ethical, legal and security issues that may arise during the project's life, as well as to set the basic ethical, legal and security requirements that need to be taken into consideration in order for SPHINX to be and remain fully compliant. **It should be mentioned that this report is delivered at an early stage of the project and any findings are of a preliminary nature. The aim is to present the main risks associated with the project and suggest the basic measures that should be undertaken by the projects' partners in order to warrant compliance in all three fields mentioned above, ethical, legal and security. In addition, many of the issues referred to hereunder are the subject of separate deliverables and therefore this analysis will be limited to a first level presentation of the ethical concerns related to SPHINX.**

In order for better evaluating the ethical and legal concerns the SPHINX project may raise, it is important to examine some of its particularities. In more detail, **two parameters should mainly be considered in the context of the SPHINX project:**

a. Its focus on the health sector;
b. Processing of special categories of data and in particular sensitive data may take place during the project execution.

As far as the first parameter is concerned, the project's description indicates that SPHINX is a cyber security tool that aims to address cyber security issues and threats in the health sector. It is unquestionable that hospitals and health care centres are prime targets for cyber criminals, especially concerning data theft, denial-of-service and ransomware. Therefore, in comparison to other cyber security solutions, SPHINX raises extra security, privacy and ethical concerns due to the sensitive character of the "market" it addresses. Issues related to vulnerable subjects (patients), informed consent as far as their participation in the project is concerned and the processing of their personal data, confidentiality (patients' confidential information), misuse of the project's findings and of course security issues are some of the parameters that will be examined below and are closely connected to the project's description and specifications.

The other parameter is directly related to the first one and refers to the processing of personal data that may take place while executing the project. Given that SPINX is focused on the health sector, special caution should be attributed to any personal data processing. In particular, SPHINX may involve the processing of special categories of personal data and more specifically health data. Again, some serious concerns regarding the lawfulness of the processing, individual consent, the rights of the individuals whose data are being processed

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 of course the security of the personal data that have been collected are some of the issues that shall be addressed in this report.

4.3 SPHINX and ethics: compliance with ethical principles

4.3.1 The European Commission's checklist

As already mentioned in section 1 of this report, identifying ethical issues and risks in research and suggest measures to minimise or prevent them and of course address them is the key to safeguard that research will indeed be conducted and completed in accordance with ethical principles and values.

Based on the Commission's guidelines on how to complete an ethics self-assessment, the first step that needs to be taken in order to make sure that the SPINX project is ethically compliant, is to check if the project falls within any of the following categories of research and if yes what extra measures should be undertaken to that direction

Does SPINX research falls within any of these categories of research?	YES	NO
• Research on human embryos and foetuses		x
• Research on human beings		x
• Research on human cells or tissues		x
• Research which involves processing of personal data	x	
• Research involving animals		x
• Research involving non-EU countries		x
• Research that may adversely affect the environment, or the health and safety of the researchers involved		x
• Research involving goods, software and technologies covered by the EU export Control regulation No 482/2009 (dual use items)		x
• Research that has an exclusive focus on civil applications	x	
• Research involving or generating materials, methods, technologies or knowledge that could be misused for unethical purposes	x	

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 1: Ethics Self-Assessment Questionnaire

Based on the above checklist the main ethical concern that is raised is the one concerning processing of personal data and potential misuse of research findings for unethical purposes. The personal data issue is addressed below under 4.4. In addition, misuse of research findings is dealt with in deliverable D1.4.

4.3.2 List of ethical issues in the SPHINX project

a) Informed consent

Acquiring informed consent from the subjects participating in a research is absolutely necessary in order to conduct research ethically. In the case of SPHINX in particular, if human subjects are required to participate in the research, it should be ensured that their consent has been validly provided in advance. Valid consent should be:

a. freely given

b. obtained in advance

c. in writing

d. based on adequate and accurate information

e. freely withdrawn

Adequate and accurate information includes the following:

The purposes of the research and information about what will happen with the results of the research.
The experimental procedures and a detailed description of the involvement of the participants, including the expected duration, and all the relevant procedures
All foreseeable risks or discomforts expected to occur for the research subjects during and after their participation
All benefits to the participants or to others which may reasonably be expected to occur
The insurance guarantees for the participants during and after participation and information on the foreseen treatments and compensations. Alternative procedures or treatments that might be advantageous to the participant need to be disclosed
Procedures in case of incidental findings
A description of the procedures adopted to guarantee the participant's privacy: the levels of confidentiality, the measures to protect the data, the duration of the storage of the data and what will happen with the data or samples at the end of the research
Contact details for researchers who can be contacted at any time to answer pertinent questions about the research and the participant's rights and that can be contacted in the event of a research related injury.

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 clear statement that the participation is voluntary, that the refusal to participate will involve no penalty or loss of benefits to which the participant would otherwise be entitled and that the participant may decide, at any time, to discontinue participation without penalty.
Information about the organisation and funding of the research project.

Table 2: Required Information needed to be provided to acquire consent

How is informed consent treated in the SPHINX project?

It is noted that informed consent forms have been circulated to the project partners. With regard to the end users/hospitals participating in the project, given that these institutions use their own consent forms, these forms have been approved and meet the above conditions.

Special attention should be given in case children or elderly people participate in the SPHINX research. In this event informed consent should be obtained from the legally authorised representative. To this effect the consent form should include a special reference to the lawful representative and his relation to the subject participate in the research.

b. Civil application and dual use

All research activities carried out under the Horizon 2020 shall have an exclusive focus on civil application. The SPHINX project has a clear civil application use. Consequently, any further elaboration on potential dual use is considered unnecessary.

c. Vulnerable subjects

Based on the definition of vulnerability and vulnerable groups respectively, as these were presented under 1.4.3 above, **the participation of people belonging to such categories in the SPHINX project is not anticipated for the project's duration**. Personal data of vulnerable groups of people may be collected, but this is another issue that is addressed separately. If human participation happens after all, given that the end users participating in the SPHINX research are hospitals and, ultimately, patients, it should be warranted that these vulnerable subjects will be treated with respect and that special attention will be attributed to their "special" situation. The vulnerability of ill people consists of different parameters that may compromise their free and conscious decision to participate in the project. For instance, advanced age, sentimental or physical condition that makes decision-making more difficult, lack of competence due to mental condition are some of the factors that may affect the free and informed decision of vulnerable subjects- in the case of SPINX patients- to participate in the research.

How could these difficulties be addressed in the SPHINX project?

- make sure that participation of vulnerable subjects in SPHINX is absolutely necessary and cannot be replaced by non-vulnerable groups;
- provide adequate information in simple wording, written in the language of the participants should be provided to them prior to their decision to participate in the SPHINX research;
- evaluate the special conditions and vulnerabilities of the participants and improve the quality of consent;
- make sure that the representative, if needed is well aware of the participant vulnerability and will act with the participant's best interest in mind (use family);

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.

- if consent is not feasible, acquire assent;
- facilitate and simplify the opt-out process (vulnerable subjects should be able to leave the research at any time and without extra formalities);
- create the environment to make the subject's participation as comfortable as possible based on his/her vulnerabilities.

d. Privacy / confidentiality

The relevant section in Chapter 1 of this report examined the notions of privacy and confidentiality and concluded that they are considered related notions in research ethics. Both definitions suggest protection of a person's life, decision-making and personal information. In the case of the SPHINX project both principles should be taken into consideration. The reason for that, as explained in the previous sections, is evidently connected to the possible involvement of (vulnerable) human subjects in the SPHINX research. Respect for privacy indicates that the participants' decision to be involved in the first place and during the research should be respected. At the same time respect for the participants' private life should always be a main concern of the researchers/ SPHINX partners. The vulnerability of the participants (ill, older people) makes this obligation even more vital, given that, on the on hand these people may be exposed to higher risk of privacy violations, (due to lack of competence or incapacity) and on the other hand any possible breach may entail serious concerns for the participants' well-being.

Confidentiality is considered an aspect of privacy and should also be respected throughout the project's life and of course after its completion. As with participants' private life, their personal information should also be treated with respect and with a high degree of confidentiality. SPHINX is a cyber security solution. As such, its main purpose is to keep the participants' information confidential. The principle of confidentiality and how it could be protected in the context of the SPHINX project is closely connected to the data protection principle and therefore it will be examined thoroughly below in the relevant section. It is however mentioned that the nature of SPHINX as a cyber security tool targeting the health sector, makes the protection of confidential (health) information a necessity. Safeguarding confidentiality reinforces trust, and trust is crucial, when the subject decides to share with the recipient his/her valuable medical information.

How could privacy/confidentiality be succeeded in the SPHINX project?

Some of the basic requirements that should be implemented in order for the principles of privacy and confidentiality to be observed are:

- the subject's informed consent should be acquired and be updated at all stages of the SPHINX project in the event of a change. The content of the informed consent is examined above under 1.4.1(d);
- the subject needs to be always aware that he/she is part of a research. Special caution should be attributed in the event that vulnerable groups of people participate in the project;
- such consent should be freely with withdrawn at all stages of the research;
- safeguard that the environment where the research takes place is appropriate. For instance, if the participants are being interviewed, that they will be able to do so in a private place;
- if family members of the participants are involved in the SPHINX research indirectly, that their privacy is also respected;
- apply data protection mechanisms (privacy by design or security by design for instance). This will be examined below under 4.4.4. and 4.4.5;
- take security measures for the protection of network and information systems. This measure will also be examined below under the relevant section (4.5.2);
- if there is the need to disclose confidential information acquire the prior written consent of the subject;
- make sure that everybody involved in the process are bound by confidentiality obligations (either by law or by virtue of a non-disclosure agreement);

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.

- take the necessary precautions to keep such information confidential even after the project has expired

e. Protection of personal data

As already pointed out, protection of personal data is a major ethic issue that needs to be addressed in all EU-funded projects. As far as the SPHINX project is concerned, the possibility of personal data being processed should be assessed. In the event that such processing takes place, specific measures should be adopted in order for the processing to be lawful and at the same time in order to safeguard the security of the personal data collected and of course the rights of the data subjects regarding their personal data.

The nature of the data that may be processed during the SPHINX project makes the data protection parameter even more crucial. In the event that personal data processing takes place, these data will, among others, include special categories of data and in particular health data. Therefore, extra requirements should apply to keep such data secure.

The measures that should be adopted in order for the SPHINX project to comply with the data protection legislation shall be thoroughly examined below under 4.4.1. In any case a detailed data protection risk assessment is highly recommended. This will help in identifying the risks related to the processing of personal data in SPHINX as well as in implementing the safest solutions in order to keep these data safe. In addition to that any data protection policies applied already by the hospitals should be brought to the attention of SPHINX.

f. Potential misuse of research findings

Given that the risk of potential misuse of the SPHINX research findings, as well as the suggested measures to minimise and address these risks are the subject of deliverable D1.4., this analysis references directly to that deliverable.

g. Information security

Information security has three dimensions: confidentiality, integrity, and availability of information. Information security plays an important role when it comes to research ethics. Keeping information, provided or generated during a project, safe, in other words safeguarding the integrity, confidentiality and availability of such information, should always be a high priority for everyone involved in research.

It has already been demonstrated that information, including valuable information, such as medical data, plays an important role in the SPHINX project. Besides the possible processing of such information, the SPHINX solution aims exactly at providing the health sector, with a security tool against possible attacks that may put (valuable) information at risk.

Information security could be achieved through the adoption of adequate organisational and technical measures. The specific measures that could be implemented in the SPHINX project are examined below under 4.5.2.

4.4 SPHINX and the protection of personal data; Compliance with the GDPR

4.4.1 Personal data processing in the context of the SPHINX Project

As elaborated above, the SPHINX project's purpose is to introduce a cyber security 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 SPHINX cybersecurity tool.

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.

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 IT health 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 care provider that will use the SPHINX solution.

With these parameters in mind, the SPHINX project falls within the scope of the GDPR and should consequently comply with its provisions.

It is pointed out that personal data processing activities conducted in the context of the SPHINX project are separately examined under Deliverable D.1.7, entitled Ethics Data Processing Activities Risk Evaluation. The present report therefore aims to make an introductory presentation of these issues, which will be further and thoroughly elaborated under the relevant deliverable.

4.4.2 Main principles on personal data processing and their application in the SPHINX project

a. The principles of article 5 (1) of the GDPR and the principle of accountability of article 5 (2)

According to article 5 of the GDPR, personal data shall be:

- processed lawfully, fairly and in a transparent manner;
- collected for a specified explicit and legitimate purpose;
- adequate, relevant and limited to the purpose of processing;
- accurate and up to date;
- stored for no longer that is necessary for the purposes of processing;
- processed in a manner that ensures security of personal data.

As far as SPHINX is concerned it is advised that the hospital or healthcare organization 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. 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 4.4.5.

According to Article 5.2 of the EU 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 provider 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 that hospitals or healthcare organization may need to comply with.

b. Lawfulness of the processing

According to Article 5.1(a) of the EU GDPR, "*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*

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.

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.

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' compliance with its obligation as a processor of personal data and in particular sensitive personal data. In this context, hospitals and health care providers that are going to implement and use 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. SPHINX shall provide hospitals with all necessary technical information in order to make such consent up to date, including processing that may take place during the SPHINX project.

c. The principle of transparency

According to the same Article 5.1(a) of the EU GDPR discussed above, personal data must also be processed in a transparent manner. Further guidance on what transparency exactly means is provided in Recital 39: *"[…] 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. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data".

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, 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 providers apply a data protection policy in order to be able at any time to provide the data subjects with the required information regarding their personal data, as these are included in articles 13 and 14 of the GDPR.

d. Informed consent

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.

According to article 7 it is the controller's obligation to demonstrate that the data subject has consented to processing of his/her personal data. Consent should be freely given and freely withdrawn at any time. If given in the context of a written declaration which also concerns other matters, the request for consent must be demonstrated in a way that is distinguishable from the other matters in an intelligible and easily accessible form, using clear and plain language.

In the context of SPHINX and given that the solution and platform shall have access to personal data of the hospitals and health centres patients, it should be ensured that a valid consent form the data subjects is always in place. The sensitive nature of the data in question (health data) makes this obligation even more significant. Hospitals should circulate informed consent forms to their patients and should always keep these forms updated. SPHINX solution assumes that, in all cases where processing of personal data is involved, a valid informed consent from the data subject has been acquired.

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

a. The right to information and access to personal data

The right to 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.

As far as SPHINX is concerned, it is advised that the hospitals and health care providers using the SPHINX Platform, in their capacity as data controllers, 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 time, etc.

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, as data controller, must inform the data subjects/patients that their personal information are being processed, provide the data subject with the 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)).

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),

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.

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 project, the hospitals, 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 apply, 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, if of course the hospital could demonstrate such legal basis.

4.4.4 The SPHINX solution and the security of the processing

Security of the processing is regulated under section 2 of the GDPR and in particular articles 32-34. Article 32 lists the measures the controller and the processor shall implement in order to ensure a level of security appropriate to the risk. These measures include among others:

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.

In addition to the organisational and technical measures another parameter for ensuring security is the process of notifying a personal data breach to the supervisory authority, as this is described in article 33 of the GDPR. 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.

How does security of processing apply to SPHINX

The SPHINX toolkit and platform aims to help organisations of the health sector to minimise cybersecurity threats and to respond to cybersecurity incidents. As a security by design solution SPHINX serves (by default) the security of processing. Users/hospitals may choose from a wide range of services available at the SPHINX security based of their needs. In other words, the SPHINX solution's purpose is focused on safeguarding the security, integrity and confidentiality of the personal data processed by hospitals by offering tailored solutions adapted to the specific needs of the IT health sector.

Regarding the hospitals themselves, it is anticipated that, in addition to the safeguards provided by the use of the SHPINX solutions, they apply a security policy and they 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 processing activities conducted by the hospitals and the health care providers make the obligation to keep such data secure of a vital importance.

4.4.5 The SPHINX solution and data protection by design

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*

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.

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".

How do these principles apply to SPHINX?

As far as SPHINX is concerned, it is the hospitals and health care providers obligation, as data controllers, to implement measures that meet the data protection by design and default principles. It is mentioned often in this report that the obligation of hospitals to comply with the GDPR's provisions is accentuated given the special character of the personal data (health data) they process. SPHNIX aims exactly at helping hospitals comply with the data protection legislation. SHPINX should therefore at the early stage of its "architectural building" take the appropriate measures in order to implement the data protection by design and by default principle. 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 Regulation etc.

4.5 SPHINX as a digital service provider: compliance with the NIS Directive

4.5.1 Is SPHINX a digital service provider?

In order to evaluate whether the SPHINX project needs to comply with the obligations set by the NIS Directive, applied to operators of essential services and digital service providers, it should be clarified whether SPHINX falls within one of these categories. SPHINX platform does not have any of the characteristics needed in order for it to be categorised as an operator of essential services (a public or private entity of a type referred to in Annex II of the Directive – energy, transport, health etc. – which provides a service that is essential for the maintenance of critical societal and/or economic activities).

The project description indicates that the SPHINX toolkit and platform can't be characterised as a digital service provider, however it lays the groundwork for a future project, that will potentially built on the findings of the SPHINX solution, and which will offer services that is very likely to attribute to SPHINX the features of a digital service provider. In particular, SPHINX could develop into an automated zero-touch device and service verification toolkit that will be easily adapted or embedded on existing, medical, clinical or health available infrastructures, whereas a user/admin will be able to choose from a number of available security services through SPHINX cyber security toolkit. The SPHINX toolkit will enable service providers to specify complete services and sell or advertise these through a secure and easy to use interface. This argument, together with the nature of the SPHINX solution itself, as a cybersecurity tool, encouraged the authors of this report to examine the cybersecurity regulatory framework during evaluation of the Project's compliance with applicable legal and ethical rules. At the same time, the nature of the organisations the SPHINX solution targets, namely hospitals and health care organisations (in other words operators of essential services) contributed further to our decision to take the cybersecurity legislation into consideration. Finally, the NIS Directive states in its Recital 58 that "this Directive should not preclude Member States from imposing security and notification requirements on entities that are not digital service providers within the scope of this Directive, without prejudice to Member States' obligations under Union law". Based on these assumptions, the aim of this section 4.5 is not to burden the Project with additional – not clearly required- compliance obligations, rather than to raise awareness on a legal framework that is very likely to prove relevant in the future.

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.

Having clarified this, we will offer a brief presentation of how the NIS Directive could be implemented on the SPHINX project, having always in mind that the SPHINX solution is not a digital service provider but it is highly anticipated to become one in the future.

In the event that the SPHINX solution becomes a digital service provider and more specifically an online marketplace, as per the definitions of Articles 6 and 4(17) of the Directive it is anticipated that it will comply with the obligations the NIS Directive imposes on digital service providers for the security of their network and information systems (security requirements and incident notification).

4.5.2 SPHINX's compliance with security requirements: Examples of security measures

The NIS Directive describes, in its Article 16, the security requirements that digital service providers should take into consideration in order to manage the risks that threaten the security of the network and information system they use in order to offer their service. More specifically, according to the first paragraph of article 16, the measures that must be adopted by digital service providers shall take into account the following elements:

a) The security of the systems and facilities;
b) Incident handling;
c) Business continuity management;
d) Monitoring, auditing and testing;
e) Compliance with international standards.

These security elements are further elaborated in the Commission's Implementing Regulation (EU) 2018/151- specifications of elements of article 16 (see above under Part A, 4.3.). It is once again noted that the Directive adopts a lighter approach when it comes to DSPs. In view of the above, SPHINX, as a future digital service provider, should comply with the Directive's provisions, in the sense that it should take all necessary measures to ensure the security of the network system it uses in the context of offering its services and consequently to protect the interests of the undertakings (hospitals, health care providers) who have access to such services.

In an effort to assist Member States and DSPs in providing a common approach regarding the security measures for DSPs, ENISA has issued technical guidelines with useful examples of such measures. Taking these into consideration, an indicative list of minimum security measures follows. More specifically, SPHINX could, in order to establish, implement, operate, monitor and continuously maintain and improve an appropriate level of security, consider and implement the following:

- perform a risk assessment (it should be performed throughout the system life cycle);
- establish and maintain an information security policy (make the key personnel aware of such policy, review the security policy following incidents, etc.);
- establish and maintain an appropriate governance and risk management framework to identify and address risks for the security of the offered services (create a list of main risks, make key personnel aware of the main risks, ensure that key personnel use the risk management methodology and tools, etc.);
- assign appropriate security roles and security responsibilities to designated personnel (personnel is formally appointed in security roles) - establish and maintain a policy with security requirements for contracts with suppliers and customers. SLAs, security requirements in contracts, outsourcing agreements (Set a security policy for contracts with third parties, perform risk analysis before entering any outsourcing agreement);
- perform background checks on personnel before hiring (Perform background checks/screening for key personnel and external contractors, when needed and legally permitted);

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.

- verify and ensure that personnel have sufficient security knowledge and that they are provided with regular security training (regularly provide key personnel with relevant training and material on security issues);
- establish and maintain an appropriate process for managing changes in personnel or changes in their roles and responsibilities (implement policy/procedures for personnel changes);
- establish and maintain policies and measures for physical and environmental security of data centers such as physical access controls, alarm systems, environmental controls and automated fire extinguishers (prevent unauthorized physical access to facilities and infrastructure, Document procedure for emergency cases);
- establish and maintain procedures for detecting and responding to security incidents appropriately (implement industry standard systems and procedures for incident detection and response);
- establish and maintain appropriate procedures for reporting and communicating about security incidents (implement relevant policy);
- establish and maintain procedures and systems for monitoring and logging of the offered services (set up tools for monitoring critical systems);
- establishes and maintains appropriate procedures for testing key network and information systems underpinning the offered services (implement tools for automated testing);
- establish and maintain a policy for checking and enforcing the compliance of internal policies against the national and EU legal requirements and industry best practices and standards (Implement policy/procedures for compliance monitoring and auditing);
- establish and maintain an appropriate policy for keeping secure the interfaces of services which use personal data. (set a high-level security policy for keeping the cloud and online market interfaces secure, make key personnel aware of the security policy.
- establish and maintain a policy which ensures that the software is developed in a manner which respects security (Establish guidelines for maintaining software security)

4.5.3 SPHINX and incident notification; Cooperation with national authorities

Incident notification is another obligation imposed on digital service providers in the context of the NIS Directive. Consequently, digital service providers need to notify to the competent authority any incidents with a substantial impact on the provision of their services. As examined above under 3.4.3 this obligation is regulated under article 16 par 3 and 4. As far as the definition of substantial impact is concerned a detailed analysis is included in section 3. In view of the above, SPHINX, as a future DSP operating in the EU, should comply with the incident notification process. ENISA in its guidelines, lists four steps that a DSP should follow when determining the impact of an incident. These steps are listed below as an indicative list of the measures that could be implemented in order to achieve compliance with the notification obligation.

STEP 1: Identify the geographical spread of the incident

At this level, a DSP should identify if the provision of the service concerned (NIS downtime) was affected within the EU political borders. If a positive result will come out, the countries affected should be identified.

Question to answer on STEP 1: Does the incident affect the proper accessibility of the service within EU?

STEP 2: Determine the extent of the disruption

The extent of the disruption must be analyzed taking into account the 4 protection goals expressed within the Directive: integrity affected (information or output provided altered), confidentiality affected (interception, unauthorized access), availability affected (service degraded, interrupted and/or unusable), authenticity affected (cannot be trusted).

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.

Question to answer on STEP 2: Is the service unavailable, unusable, or unsafe to use due to the incident?

STEP 3: Determining the Usertime

The two parameters “number of users affected” and “duration of the incident” were merged into a single one entitled Usertime.

Question to answer on STEP 3: Does the impairment caused by the incident is above the absolute or relative thresholds in terms of Usertime?

4. STEP 4: Determining the extent of the impact on economic and societal activities

The overall purpose of the NISD is to protect the internal market from damages produced by cyber-incidents. Identifying the real economic and societal impact for every incident is challenging for both DSPs and national authorities, as most of the information needed resides outside their organizations. Therefore, this is mainly an estimative exercise aiming at giving the EU authorities a glimpse into the potential disruptive effects upon the internal market and EU citizens. In this respect, the approach pro-posed in step 4 is based on predefined levels of affected users: The more users are affected the bigger the potential impact.

It is noted that SPHNIX as a future digital service provider shall be obliged to notify an incident only in those cases where it has access to the information needed to assess the impact of such incident (article 16 (4) of the NIS Directive). If this is the case, SPHNIX shall notify the competent authority or the CSIRT, designated by the Member State where SPHINX has its main establishment, without undue delay of any incident having a substantial impact on the provision of its services. Notifications shall, according to article 16(3) of the NIS Directive include information to enable the competent authority or the CSIRT to determine the significance of any cross-border impact. According to article 17 of the NIS Directive Member States shall ensure that the competent authorities take action, if necessary, through **ex post** supervisory measures, when provided with evidence that a digital service provider does not meet the requirements laid down in Article 16. Such evidence may be submitted by a competent authority of another Member State where the service is provided.

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) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC

ALLEA – All European Academies, The European Code of Conduct for Research Integrity,

http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf

Charter of Fundamental Rights of the European Union,

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN

Council of Europe, Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine,

https://rm.coe.int/168007cf98

Council Regulation No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual use items

European Commission, Horizon 2020 Programme, Guidance: How to complete your ethics self-assessment,

https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_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

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

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

European Commission, Guidance Note – Research with an exclusive focus on civil applications

https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-civil-apps_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.

European Commission, Guidance Note: Potential Misuse of Research (& Explanatory Note)

https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-misuse_en.pdf

https://ec.europa.eu/research/participants/portal/doc/call/h2020/fct-16-2015/1645168-explanatory_note_on_potential_misuse_of_research_en.pdf

European Convention of Human Rights

https://www.echr.coe.int/Documents/Convention_ENG.pdf

European Commission, Ethics and Data Protection,

https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf

ENISA, Guidelines for SMEs on the security of personal data processing

https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

ENISA, Incident notification for DSPs in the context of the NIS Directive

https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of- the-nis-directive

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.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L1535

United Nations, Universal Declaration of Human Rights

https://www.un.org/en/universal-declaration-human-rights/

Framework Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services

Regulation 910/2014 on electronic identification and trust services for electronic transactions in the Internal market and repealing Directive 1999/93/EC

Commission Implementing Regulation (EU) 2018/151, of 30 January 2018, laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of

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.

network and information systems and of the parameters for determining whether an incident has a substantial impact.

Directive 2013/11/EU of the European Parliament and of the Council on attacks against information systems and replacing Council framework Decision 2005/222/JHA

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.