D1.5 Ethics Manual and Guidelines for information security in the Health Sector

WP1– Project Management

Version: 1.00

SPHINX

A Universal Cyber Security Toolkit for Health-Care Industry

Disclaimer

Copyright message

Document information

Grant Agreement Number	826183	Acronym	SPHINX
Full Title	A Universal Cyber Security Toolkit for Health-Care Industry		
Topic	SU-TDS-02-2018 Toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures		
Funding scheme	RIA - Research and Innovation action		
Start Date	1st January 2019	**Duration**	36 months
Project URL	http://sphinx-project.eu/		
EU Project Officer	Reza RAZAVI (CNECT/H/03)		
Project Coordinator	National Technical University of Athens - NTUA		
Deliverable	D1.5. Ethics Manual and Guidelines for information security in Health Sector		
Work Package	WP1 – Project Management		
Date of Delivery	**Contractual** M9	**Actual**	M9
Nature	R - Report	**Dissemination Level**	P - Public
Lead Beneficiary	NTUA		
Responsible Author	Christos Ntanos	**Email**	cntanos@epu.ntua.gr
		Phone	
Reviewer(s):	Vagelis Papakonstantinou [VUB-LSTS], Ricardo Cabecinha [HES]		
Keywords	Information security, Ethics		

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	19/07/2019	Draft	ToC	George Doukas (NTUA)
0.20	29/08/2019	Draft	Contributions to Sections 2,3 & 4	George Doukas (NTUA)
0.30	03/09/2019	Draft	First Draft	George Doukas (NTUA)
0.40	24/09/2019	Draft	Contribution to Section 2	Sergiu Marin (Polaris Medical) Dana Oniga (SIVECO)
0.50	24/09/2019	Draft	Final draft submitted for review	George Doukas (NTUA)
0.60	27/09/2019	Draft	Review 1	Vagelis Papakonstantinou (VUB-LSTS)
0.70	27/09/2019	Draft	Review 2	Ricardo Cabecinha (HESE)
0.8	29/09/2019	Pre-final	Incorporated review comments, content completion	George Doukas (NTUA)
0.81	29/09/2019	Pre-final	Quality Control	Christos Ntanos (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

The Sphinx project aims to provide a Universal Cyber Security Toolkit for the Health and Care Domain. This deliverable outlines the basic steps for the implementation of the information security strategy within health sector. Provided that Sphinx R&D activities should comply with established practices as well as the legal framework for ethical, privacy and data protection issues, the deliverable identifies restrictions and provides guidelines in relation to privacy and data protection as well as access to personal information. The goal is to ensure that the project methods, tools, technologies and processes will be able to be adopted without any legal barrier at least as this concerns the national (three pilots) and the European legal and ethical framework and mainly 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.

Contents

1 Introduction 7

1.1 Purpose & Scope 7

1.2 Structure of the deliverable 7

1.3 Relation to other WPs & Tasks 7

1.4 List of Abbreviations 8

2 Legal Framework 9

2.1 European Legislation 9

2.1.1 The right to private life and data protection 9

2.1.2 General Data Protection Regulation 11

2.2 National Legislation 30

2.2.1 Greece 30

2.2.2 Portugal 34

2.2.3 Romania 37

3 Information Security for the Health Care Sector 41

3.1 Information security Framework 42

3.1.1 Information security policy 42

3.1.2 Specifying Roles & Responsibilities 43

3.1.3 Framework Review 43

3.1.4 Additional Safeguards 43

3.2 Risk Management 44

3.2.1 Objective 44

3.2.2 Risk Assessment 44

3.2.3 Risk Treatment 45

3.2.4 Risk Monitoring & Reviewing 46

4 Regulations and Platform-related Ethical Aspects 47

4.1 Compliance with the current national and EU legislation 47

4.1.1 Agreements, laws and regulations (including EU directive on data protection) 47

4.2 Acquiring agreements with third parties 47

4.3 Platform-related Ethical aspects 47

4.3.1 Applying privacy design principles-ensuring appropriate level of sensitive personal data protection 47

4.3.2 Ensuring prevention of platform misuse (by any potential stakeholder of the platform) 48

4.3.3 Transparent administration of log files (content; protection; access; destruction) 48

4.3.4 Pre-define aspects of platform maintenance 48

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.

5 Ethical Provisions within Sphinx 49
5.1 Identify/recruit Research participants 49
5.2 Ensuring data minimisation principle 50
5.3 Informed Consent 50
5.4 Terms of Use 50
5.5 Code of Ethics of professionals that provide and administrate information 50
5.6 Detailed instructions for data sharing 51
5.7 Safeguarding users' privacy and confidentiality of personal data 51
5.7.1 Inform users about what personal information might be accessed, collected, how and why the information will be used and how they can control this use 51
5.8 Privacy policy 51
6 Summary and Conclusions 53

Table of Tables

Table 2-1: Key GDPR points 13
Table 2-2: Basic principles of personal data (PD) processing – Article 5 GDPR 16

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 Introduction

1.1 Purpose & Scope

The Sphinx project aims to provide a Universal Cyber Security Toolkit for the Health and Care Domain. The proposed toolkit will be an embedded, smart and robust security awareness layer, able to identify modern and advance cyber threats, enhanced with a personalised data security management tool. Novel methodologies for harnessing and integrating multisource information will be designed, along with the application of profiling techniques, predictive algorithms, and end-to-end data privacy methods.

This deliverable outlines the basic steps for the implementation of the information security strategy within health sector. Provided that Sphinx R&D activities should comply with established practices as well as the legal framework for ethical, privacy and data protection issues, the deliverable identifies restrictions in relation to privacy and data protection as well as access to personal information. The goal is to ensure that the project methods, tools, technologies and processes will be able to be adopted without any legal barrier at least as this concerns the European legal and ethical framework and mainly the GDPR.

Thus the deliverable includes the state-of-play of data protection, privacy and ethical issues related to the processing of personal data as this will take place in the activities of Sphinx.

1.2 Structure of the deliverable

The deliverable is structured as follows:

In Section 1, an introductory description of the document is provided, communicating its scope, its structure and its relation to other WPs and tasks of the project. The final chapter of the section includes a table with all abbreviations appearing in the document.

In Section 2, the European and national legal framework related to personal data retrieval, processing and management is presented mainly focusing on the GDPR.

In Section 3, the general approach for the implementation of the information security strategy within the health sector is presented.

In Section 4, general ethical aspects related to regulations and technical aspects of Sphinx are presented focusing on compliance with current legislation, agreements with third parties and other pertinent matters.

Section 5 includes ethical provisions related to non-technical aspects of individual functional components of Sphinx. As such, it focuses on the steps that must be taken to form the terms of use and privacy policy of the platform and other relevant aspects.

Section 6 concludes the document.

1.3 Relation to other WPs & Tasks

The present deliverable is released within the context of Work Package 1 “Project Management”. Deliverables D1.3 to D1.8 & D1.10 provide information about the type and the exploitation of collected data and the GDPR framework. In these deliverables an analytical description of how the Sphinx project implements the GDPR regulations is included, the processing activities of the personal data that might take place in the Sphinx platform, and how the use of state of the art technologies will protect the rights of end-users in general.

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.

1.4 List of Abbreviations

The following table includes all abbreviations used in the document.

GDPR	General Data Protection Regulation
DMP	Data Management Plan
CoE	Council of Europe
CETS	Council of Europe Treaty Series
Charter	Charter of Fundamental Rights of the European Union
HDHR	Universal Declaration of Human Rights
TFEU	Treaty on the Functioning of the European Union

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 Legal Framework

2.1 European Legislation

2.1.1 The right to private life and data protection

For the first time, a right to protection of an individual's private sphere against intrusion from others, especially from the state, was established in Article 12 of the United Nations Universal Declaration of Human Rights (UDHR) of 1948 on respect for private and family life[1]. Thereafter, European legal instruments have been influenced and established. The right to data protection evolved out of the right to respect for private life.

The European Convention on Human Rights

The Council of Europe, as it was formed in the aftermath of the Second World War, adopted the European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights - ECHR)[2] in 1950, which entered into force in 1953[3]. ECHR sets forth a number of fundamental rights and freedoms (right to life, prohibition of torture, prohibition of slavery and forced labour, right to liberty and security, right to a fair trial, no punishment without law, right to respect for private and family life, freedom of thought, conscience and religion, freedom of expression, freedom of assembly and association, right to marry, right to an effective remedy, prohibition of discrimination). More rights are granted by additional protocols to the Convention. It is noteworthy that, under the Lisbon Treaty, fundamental rights, as guaranteed by the ECHR and as they result from the constitutional traditions of the Member States, constitute the general principles of the Union's law[4].

Under the ECHR the right to protection of personal data is guaranteed in Article 8 as part of the right to respect for private and family life, home and correspondence and lays down the conditions under which restrictions of this right are permitted, such as when in accordance with law and in the interests of public security and public safety, for the prevention of disorder or crime, for the protection of rights and freedoms of others.

Council of Europe Convention 108

In need for the development of more detailed rules to safeguard individuals by protecting their personal data and following a series of resolutions that were adopted by the Committee of Ministers of the Council of Europe,[5] in 1981 the Convention for the protection of individuals with regard to the automatic

[1] United Nations (UN), Universal Declaration of Human Rights (UDHR), 10 December 1948, available at: http://www.un.org/en/universal-declaration-human-rights/index.html .

[2] CoE, European Convention on Human Rights, CETS No. 005, 1950, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005.

[3] States have an international obligation to comply with the ECHR and to this end, the European Court of Human Rights (ECtHR), was set up in 1959, where complaints from individuals, groups of individuals, NGOs or legal persons and States alleging violations of the Convention are received and considered to ensure the observance of the engagements undertaken by the Parties. To date, the Council of Europe comprises of 47 member states, out of which are 28 EU member states;

[4] Article 1 of the Lisbon Treaty amending article 6 para 3 of the Rome Treaty.

[5] Resolution (73) 22 on the protection of the privacy of individuals *vis-à-vis* electronic data banks in the private sector, 26 September 1973; CoE, Committee of Ministers (1974), Resolution (74) 29 on the protection of the privacy of individuals *vis-à- vis* electronic data banks in the public sector, 20 September 1974).

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 of personal data (Convention 108)[6] was opened for signature[7]. Convention 108 applies to all data processing carried out by both the private and public sector, here including the judiciary and law enforcement authorities and seeks to regulate the trans-border flow of personal data. It lays down principles for the collection and processing of personal data in order to protect the individual form abuses during these process, namely fair and lawful collection and automatic processing of data, storage for specified legitimate purposes (legitimacy) and for the time necessary and appropriate and use compatible with the legitimate purposes. Data processed shall be adequate, relevant, proportionate to the purpose and accurate (quality of data; proportionality). At the same time, 'sensitive data', such as a person's race, politics, health, religion, sexual life or criminal record are excluded from collection and processing, unless the necessary legal requirements are met. Moreover, under the Convention the individual has the right to be aware that information is stored on him or her and, if necessary, to react (transparency and free, specific and informed consent). Restrictions on the provided rights are possible only in case of overriding interests, such as state security or defence, are at risk.

In 2017 the Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data issued the Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data[8]. These comprise of recommendations to state parties to the Convention, controllers and processors to undertake measures related to data protection for the prevention of potential negative impact of the use of Big Data[9] on human dignity, human rights and fundamental freedoms. The purpose is to limit the risks for data subjects' rights, such as the potential bias of data analysis, the underestimation of the legal, social and ethical implications of Big Data on decision-making processes (e.g. mere de-contextualised information being the grounds of a decision), and the marginalisation of an effective and informed involvement by individuals in these processes (e.g. in case of power imbalance between controller and data subject). Finally, modernisation proposals for the Convention 108 have been elaborated since 2013 transmitting a draft amending protocol in 2016, which was finally opened for signature in 2018[10]. The aim of the Protocol of amendment is to modernise and improve the Convention (ETS No. 108), taking into account the new challenges to the protection of individuals with regard to the processing of personal data which have emerged since the Convention was adopted in 1981. Some of the innovations contained in the Protocol are the following:

- Stronger requirements regarding the proportionality and data minimisation principles, and lawfulness of the processing;
- Extension of the types of sensitive data, which will now include genetic and biometric data, trade union membership and ethnic origin;
- Obligation to declare data breaches;
- Greater transparency of data processing;
- New rights for the persons in an algorithmic decision making context, which are particularly relevant in connection with the development of artificial intelligence;

[6] CETS No. 108, 1981, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 . In 1999, Convention 108 was amended to enable the EU to become a Party (see Art. 23 (2) of the Convention 108 in its amended form). In 2001, an Additional Protocol to Convention 108 was adopted, introducing provisions on transborder data flows to non-parties (third countries) and on the mandatory establishment of national data protection supervisory authorities; available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181 . Note: Greece and Belgium have not ratified the Protocol.

[7] Up to date, all 47 members of the Council of Europe have ratified the Convention and 4 non-members of the CoE. Convention 108 is the only legally binding international instrument in the data protection field.

[8] Available at: https://rm.coe.int/16806ebe7a

[9] Therein the term Big Data encompasses both Big Data and Big Data analytics. Big Data are identified as extremely data sets with heterogeneous characteristics that may be analysed computationally to extract inferences about data patterns, trends and correlations; Guidelines, p.2

[10] CETS No. 223, 2018, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/

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.

- Stronger accountability of data controllers;
- Requirement that the "privacy by design" principle is applied;
- Application of the data protection principles to all processing activities, including for national security reasons, with possible exceptions and restrictions subject to the conditions set by the Convention, and in any case with independent and effective review and supervision;
- Clear regime of trans-border data flows;
- Reinforced powers and independence of the data protection authorities and enhancing legal basis for international cooperation.

European Union data protection law

EU law is composed of primary EU law, namely Treaty on European Union (TEU)[11] and the Treaty on the Functioning of the European Union (TFEU - Lisbon Treaty)[12] and secondary EU law, i.e. regulations, directives and decisions of the EU.

The Charter of Fundamental Rights of the European Union

In 2000 the Charter of Fundamental Rights of the European Union (Charter)[13] was proclaimed[14] by the EU. Tough a political document at first, the Charter became legally binding as EU primary law with the coming into force of the Lisbon Treaty in 2009[15].

The rights enshrined in the Charter are divided into six sections: dignity, freedoms, equality, solidarity, citizens' rights and justice. The Charter guarantees the respect for private and family life[16], and explicitly raises the level of data protection to that of a fundamental right in EU law by establishing the right to data protection[17]. It refers to key data protection principles, such as fair processing and for specific purpose, individual's consent or based on other legal basis[18], and ensures that an independent authority will control the implementation of these principles[19].

2.1.2 General Data Protection Regulation

Under article 16 of the TFEU, where the right to protection of personal data is safeguarded, the competency of the European Parliament and the Council to legislate on data protection matters is foreseen[20]. The principal EU legal instrument on data protection is the Regulation (EU) 2016/279 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection

[11] Consolidated version of the TEU available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012M/TXT

[12] Consolidated version of the TFEU available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12007L%2FTXT

[13] EU (2012), Charter of Fundamental Rights of the European Union, OJ 2012 C 326, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[14] Namely, at that time, it was not incorporated into the Treaty and was not legally binding.

[15] All amendments available here: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12007L/TXT

[16] Art. 7: "Everyone has the right to respect for his or her private and family life, home and communications."

[17] Art. 8(1): "Everyone has the right to the protection of personal data concerning him or her."

[18] Art. 8(2): "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."

[19] Article 8(3): "Compliance with these rules shall be subject to control by an independent authority."

[20] TFEU, Art. 16(2), available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=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.

Regulation – GDPR)[21]. By this Regulation, Directive 95/46/EC (Data Protection directive)[22] was repealed and GDPR came into force on 25 May 2018. As stipulated in the recitals of the GDPR, while a high level of natural persons' protection must be ensured with regards to the personal data processing, this should be balanced against other fundamental rights in accordance with the principle of proportionality. The technological developments and the expansion of data processing and sharing made it imperative upon the Union bodies that a strong and more coherent data protection framework should be established. Thus, a homogenous application of law throughout the EU could only be established with an EU regulation[23].

Key GDPR points[24]

Citizens' rights

The GDPR strengthens existing rights, provides for new rights and gives citizens more control over their personal data. These include:

- **easier access to their data** — including providing more information on how that data is processed and ensuring that that information is available in a clear and understandable way;
- **right to data portability** — making it easier to transmit personal data between service providers;
- **right to erasure** ('right to be forgotten') — when an individual no longer wants their data processed and there is no legitimate reason to keep it, the data will be deleted;
- **right to know when their personal data has been hacked** — companies and organisations will have to inform individuals promptly of serious data breaches. They will also have to notify the relevant data protection supervisory authority.

Rules for businesses

The GDPR is designed to create business opportunities and stimulate innovation through a number of steps including:

- **a single set of EU-wide rules;**
  a data protection officer, responsible for data protection, will be designated by public authorities and by businesses which process data on a large scale;
- **one-stop-shop** — businesses only have to deal with one single supervisory authority (in the EU country in which they are mainly based);
- **EU rules for non-EU companies** — companies based outside the EU must apply the same rules when offering services or goods, or monitoring behaviour of individuals within the EU;
- **innovation-friendly rules** — a guarantee that data protection safeguards are built into products and services from the earliest stage of development (data protection by design and by default);
- **privacy-friendly techniques** such as pseudonymisation (when identifying fields within a data record are replaced by one or more artificial identifiers) and encryption (when data is coded in such a way that only authorised parties can read it);
- **removal of notifications** — the new data protection rules will scrap most notification obligations and the costs associated with these. One of the aims of the data protection regulation is to remove obstacles to free

[21] General Data Protection Regulation, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1522240823531&from=EN

[22] Data Protection Directive, OJ 1995 L 281, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046 .

[23] "Regulations are of general application, binding in their entirety and directly applicable. They must be complied with fully by those to whom they apply (private persons, Member States, Union institutions). Regulations are directly applicable in all the Member States as soon as they enter into force (on the date stipulated or, failing this, on the twentieth day following their publication in the Official Journal of the European Union) and do not need to be transposed into national law.

They are designed to ensure the uniform application of Union law in all the Member States. Regulations supersede national laws incompatible with their substantive provisions."; information retrieved from 'Sources and Scope of European Union Law', Fact sheets in the European Union - 2018, available at: http://www.europarl.europa.eu/ftu/pdf/en/FTU_1.2.1.pdf

[24] Retrieved from: Protection of personal data, Regulation (EU) 2016/279, Summary of legislation, available at: http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32016R0679&qid=1522240823531

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.

flow of personal data within the EU. This will make it easier for businesses to expand; • **impact assessments** — businesses will have to carry out impact assessments when data processing may result in a high risk for the rights and freedoms of individuals; • **record-keeping — SMEs[25] are not required to keep records of processing activities, unless the processing is regular or likely to result in a risk to the rights and freedoms of the person whose data is being processed.**

Table 2-1: Key GDPR points

2.1.2.1 Definition & Scope

GDPR lays down rules for the protection of natural persons[26], irrespective of their nationality or residence, regarding the processing of their personal data and rules relating to the free movement of personal data (Article 1). Particularly, it applies to the processing of personal data wholly or partly by automated means, as well as by other than automated means when the personal data form or are intended to form part of a filing system (Article 2). Furthermore, with regard to the territorial scope of the GDPR[27], it applies to processing of personal data by an establishment[28] of a controller or a processor in the Union, whether a branch or a subsidiary with legal personality[29]; the processing of data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to offering goods or services to such data subjects, irrespective of payment[30]; the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, when it is related to the monitoring of the behaviour of such data subjects in so far this behaviour takes place within the Union[31].

Noteworthy that anonymous information, namely information that cannot be attributed to an identified or identifiable natural person or personal data that have become anonymous by making the data subject no longer identifiable, including for statistical or research purposes, are not regulated by the GDPR. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria do not fall within the scope of the GDPR[32]. Moreover, the processing of personal data by private individuals for merely personal or household purposes falls also out of the scope of this Regulation (household exemption)[33]. GDPR does not apply for the processing of the personal data by the Union institutions, bodies and offices and agencies, as this falls under the scope of Regulation (EC) 45/2001. In addition, with regard to processing by the judiciary and law enforcement authorities concerning the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, Directive (EU) 2016/680 applies.

[25] Small and medium-sized enterprises

[26] And not deceased; Recital 27.

[27] Art. 3 GDPR

[28] According to Art. 4(16) of the GDPR, "'main establishment' means:
(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;
(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;"

[29] Recital 22

[30] Recital 23

[31] Recital 24

[32] Recital 15

[33] Recital 18

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.

Under article 4 of the GDPR,

'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified directly or indirectly, particularly by reference to an identifier such as name, ID number, location data (e.g. GPS), online identifier via devices, applications, tools and protocols (e.g. cookies, IP address, radio frequency identification tag)[34] or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (para 1); Personal data which have undergone pseudonymisation and thus could be attributed to a natural person with the use of additional information, should be regarded as information of an identifiable person[35]. To ascertain that, objective factors should be taken into account, such as the costs and the time required for identification, as well as the available technology at the time of processing[36].

Through the use of modern technology traces might be left, which when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them[37].

'processing' 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 (para 2);

'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements (para 4);

'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 that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (para 5);

'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis (para 6);

'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 national law, the controller or the specific criteria for its nomination may be provided for by Union or national law (para 7);

'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (para 8);

'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. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or national law shall not be regarded

[34] See also recital 30
[35] Recital 2
[36] Ibid.
[37] Recital 30

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.

as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing (para 9);

'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data (para 10);

'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 (para 11);

'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (para 12);

'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result from the analysis of a biological sample from the natural person in question (e.g. DNA or RNA analysis)[38] (para 13);

'**biometric data'** means personal data resulting from specific technical processing relating to the physical, physio- logical or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data (para 14);

'**data concerning health'** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status[39] (para 15).

2.1.2.2 Basic principles of processing personal data

Basic principles of personal data (PD) processing – Article 5 GDPR
✓ **Lawfulness, fairness and transparency –** PD processed lawfully, fairly and in a transparent manner in relation to the data subject; ✓ **Purpose limitation –** PD collected for specific, concrete and legitimate purposes and any further process must be compatible with these purposes[40]; ✓ **Data minimisation –** adequate, relevant and limited to what is necessary to the purposes for which they are processed; ✓ **Accuracy –** ensure that PD are accurate and, where necessary, kept up to date; PD that are inaccurate shall be erased or rectified without delay; ✓ **Storage limitation –** PD shall be kept in a form that permits the identification of the data subject solely for the time necessary for the purpose for which the PD are processed[41]; ✓ **Integrity and confidentiality –** during processing security of PD, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, shall be

[38] See also recital 34 GDPR

[39] E.g. according to Recital 35 GDPR, "a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test".

[40] Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (art. 5(b)). See also art. 89(1) GDPR.

[41] Personal data may be stored for longer periods only if they are intended to be processed 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 in order to safeguard the rights of the data subject (Article 5 point (e)).

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

	ensured, by undertaking appropriate technical and organisational measures
✓	**Accountability -** The controller shall be responsible for, and be able to demonstrate compliance with the aforementioned principles

Table 2-2: Basic principles of personal data (PD) processing – Article 5 GDPR

The principle of lawfulness requires that personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by GDPR or other EU or national law[42] (article 6).

Other legitimate basis, according to article 6 points (b) – (f), includes:

- the necessity for compliance with the legal obligation to which the controller is subject[43];
- the necessity for the performance of a contract to which the data subject is party or as step prior to entering into a contract at the request of the data subject;
- the necessity for the protection of the vital interests of the data subject or of another natural person[44];
- the necessity according to the legitimate interests pursued by the controller or by a third party[45], unless the interests or fundamental rights of the data subject, especially where he/she is a child, which require protection of personal data, transcend[46].

Based on the European Court of Human Rights case-law, the limiting of the fundamental right to protection of personal data must be strictly necessary[47]. 'Necessity shall be justified on the basis of objective evidence and is the first step before assessing the proportionality of the limitation'[48]. Moreover, the means of processing, the categories of data processed and the duration of data storage shall be necessary for the purpose of the processing[49]. Proportionality requires that the disadvantages for not fully exercising the right to data protection do not override the advantages due to limiting the right, namely the limitation should be justified and accompanied by safeguard measures[50]. A prerequisite is that 'the measure is adequate to achieve the envisaged objective' and that only adequate and relevant personal data for the purposes of processing are collected and processed[51].

The purposes for personal data processing should be compatible with the purposes for which the personal data were initially collected and thus common legal basis covers both cases[52]. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority that the controller holds, EU or national law shall determine and specify the tasks and purposes for which the

[42] Art. 6 GDPR.

[43] "This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing." Recital 45 GDPR

[44] This should take place principally only where the processing cannot be established on another legal basis; Recital 46 GDPR.

[45] "At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place"; Recital 47 GDPR. Under Recital 49 GDPR, processing of personal data, where this is strictly necessary and proportionate for the purposes of ensuring network and information security, corresponds to a legitimate interest of the data controller.

[46] The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing"; Recital 47 GDPR

[47] European Data Protection Supervisor, Necessity & Proportionality, available at: https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en

[48] Ibid.

[49] Ibid.

[50] Ibid.

[51] Ibid.

[52] Recital 50(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.

further processing should be regarded as compatible and lawful. Where the data subject has given consent or the processing is based on Union or national law and constitutes a necessary and proportionate measure in a democratic society to safeguard, particularly, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes[53]. Yet, further processing of personal data should be compatible with legal, professional or other binding obligation of secrecy[54].

Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. However, appropriate safeguards should be in place, for example pseudonymisation. Specific provisions are foreseen under article 89 and these are thoroughly described in recitals 156-162.

The *principle of transparency* requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language or even visualisation be used[55], especially for information addressed to a child[56]. Information should be provided in writing or by other means, including electronic means. When information is provided orally, the identity of that data subject must be proven by other means[57].

Accountability corresponds to the active implementation of measures by controllers to promote and safeguard data protection in their processing operations. Controllers are responsible for the compliance of their processing activities with the GDPR and should be able at any time to demonstrate compliance to the general public and to supervisory authorities[58].

Processing of special categories of personal data[59]

- Under Recitals 51-54 of the GDPR, it is highlighted that there are personal data which are particularly sensitive in relation to fundamental rights and freedoms and for this reason these require specific protection, as the context of their processing could create significant risks[60]. These data include 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[61]. Processing of such personal data should be prohibited, unless it meets concrete conditions, such as the following[6263]:
  a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes[64];

[53] Recital 50(2)
[54] Recital 50(2)
[55] Art 13(1). Such information could be provided in writing or electronic form, for example, when addressed to the public, through a website; Recital 58.
[56] Recital 58
[57] Art. 12(1)
[58] See accordingly, European Union Agency for Fundamental Rights (FRA), Handbook on European data protection law, 2014, p.75, available at: http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf
[59] Art. 9 and Recital 51-54
[60] See particularly Recital 51
[61] Art. 9
[62] Art. 9(2)
[63] According to art. 9(4) of the GDPR, 'Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health'.
[64] except where EU or national law provide that the prohibition may not be lifted by the data subject; GDPR, Article 9(2) point (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.

b) processing is based on obligation and specific right of the controller or of the data subject in the field of employment and social security and social protection law and is established in EU or national law or a collective agreement pursuant to national law providing for appropriate safeguards for the fundamental rights and interests of the data subject[65];

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 by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim within its legitimate activities and concerns solely the members or former members of the body or persons having regular contact with it in relation to its purposes and the personal data are not disclosed outside that body without data subjects' consent;

e) processing concerns 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 on the basis of substantial public interest according to EU or national law, which shall be proportionate to the aim pursued, respect the right to data protection and provide for measures to safeguard the data subject's fundamental rights and interests;

h) processing is necessary for health-related purposes for the benefit of natural purposes and society as a whole, such as 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 EU or national law or pursuant to contract with a health professional who is bounded by professional secrecy[66];

i) processing is necessary for reasons of public interest in the area of public health on the basis of EU or national law which provides for measures to secure the rights and freedoms of the data subject, particularly 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) GDPR based on EU or national law which shall be proportionate to the aim pursued, respect the right to data protection and provide for measures to safeguard the data subject's fundamental rights and interests.

- Processing of personal data concerning criminal convictions and offences, or related security measures will only be possible when conducted under the control of a public authority or when this is based on EU or national law and appropriate safeguards are in place[67].

2.1.2.3 Consent

Consent, as examined above, is, in numerous cases, the legal basis for legitimate data processing. Consent must be free, informed, specific and unambiguous; it should be a clear affirmative act indicating the data subject's acceptance of the proposed processing of his/her personal data, in the form of a written statement or an electronic form or an oral statement (e.g. ticking a box when visiting a website, choosing

[65] See also recital 52.
[66] See also art. 9(3) and recital 53.
[67] Art. 10.

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.

technical settings for information society services).[68] Especially where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data[69]. Therefore, a declaration of consent pre-formulated by the controller should be provided in a comprehensible and easily accessible form, using clear and plain language and it should not contain unfair terms, ensuring that the data subject is aware and particularly of the extent to which consent is given[70]. In addition, in the case of a written declaration including other matters as well, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters'[71]. Any part that does comply with the GDPR rules is not binding[72].

For consent to be informed, the data subject should know at least the identity of the controller and the purposes of the processing[73]. At the same time, consent should not be regarded as freely given, not unless the data subject has genuine or free choice or is able to refuse or withdraw consent without detriment[74]. The data subject should be informed prior to giving his/her consent that he/she is able to withdraw at any time[75]; the procedure should be as easy as giving consent[76]. In addition, for consent to be freely given, it requires that it allows separate consent to be given to different personal data processing operations[77]. Furthermore, in case of contract performance or service provision, these must not be conditional on the consent for processing, if this is not a prerequisite for the performance of the contract or service[78]. Where there is clear imbalance between the controller and the data subject, it should be presumed that consent is not given freely and thus consent should be the legal basis for processing[79].

Under the GDPR, it is acknowledged that children should be granted specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards at stake, as well as their rights with regard to the processing of personal data[80]. This is especially apparent as concerns the field of marketing and information society services[81]. On that account, a child shall be at least 16 years old to consider the consent lawful[82]. For children below the age of 16 years, consent is given or authorised by the holder of parental responsibility over the child[83] and the controller should make reasonable efforts to

[68] Recital 32.
[69] Art. 7(1); Recital 42
[70] Recital 42; see also Council Directive 93/13/EEC (1)
[71] Art. 7(2) GDPR
[72] Art. 7(2)
[73] Recital 43
[74] Recital 42
[75] Art. 7(3). Note: According to art.7(3), 'the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal'.
[76] Art. 7(3)
[77] Recital 43
[78] Recital 43
[79] Recital 43
[80] Recital 38
[81] According to point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council, 'Information society service'95 means 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; Art.4(25) GDPR. Examples are: web shops and marketplaces, search engines, online advertising, video sharing sites, blogs, hosting, video-on-demand, online consultancy, online marketplaces, social networking, etc.
[82] Art. 8(1)
[83] Ibid.

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 that[84]. By contrast, in the context of preventive or counselling services offered directly to a child, the consent of the holder of parental responsibility should not be necessary[85].

2.1.2.4 Responsibilities of the controller, the processor & the data protection officer

Responsibility of the controller

The controller is responsible for the implementation of appropriate technical and organisational measures to secure and be able to demonstrate that processing is performed according with the GDPR by taking into account the context and purpose of processing as well as the impact that this might have on the rights and freedoms of natural persons[86]. These measures may include data protection policies[87] or the application of approved codes of conduct or certification mechanisms[88]. Where two or more controllers define together the purpose and means of the processing, they are joint controllers with concrete responsibilities to comply with the GDPR[89]. This arrangement should be available for the data subject too[90].

Where the controller delegates a processor to perform the processing of personal data and to act on behalf of the controller, the latter must use only processors providing sufficient guarantees to implement suitable technical and organisational measures in compliance with the GDPR and with respect to the data subject's rights[91].

Each controller, or representative of a controller in the EU, with regard to enterprises or organisations employing more than 250 persons, is responsible for keeping a record of the processing operations, in writing including in electronic form[92]. This record shall be available upon request of the supervisory authority[93]. The obligation to keep a record applies to organisations with less than 250 employees, where processing is likely to result in a risk to the data subject's rights, the processing is not occasional, or it includes personal data revealing sensitive information about an individual or relate to criminal convictions[94].

The controller is anticipated to cooperate with the supervisory authority upon request[95]. Nevertheless, in case of a personal data breach, the controller has to notify the supervisory authority within 72 hours after having become aware of the breach, expect for breaches that are unlikely to result in a risk to the data subject's rights[96]. If the notification takes place later than 72 hours, the reasons for this must be made known[97]. In the notification 'the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned' should be described; 'the name and contact details of the data protection officer or other contact point where more information can be obtained' should be

84 Art. 8(2)
85 Recital 38
86 article 24, para 1.
87 Art. 24 para 2.
88 Art. 24(3). See also articles 40 & 42 GDPR.
89 Art. 26(1).
90 Art. 26(2).
91 Art. 28(1).
92 Art. 30 paras 1,3,5.
93 Art. 30(4).
94 See articles 9(1) & 10.
95 Art. 31.
96 Art. 33(1).
97 Ibid.

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.

communicated; 'the likely consequences of the personal data breach' should be described; as well as 'the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects' should be described[98]. The controller is responsible for documenting any personal data breaches (facts relating to the breach, effects and remedial measures taken) in order for the supervisory authority to verify compliance with GDPR provisions[99].

The controller is responsible for communicating a personal data breach to the data subject, using a clear and plain language, if it is likely to affect negatively the natural person's rights[100]. If measures have been taken, such as encryption or other, that either render personal data intelligible or the risk no longer exists, the controller does not have to inform the data subject[101]. In case, it demands disproportionate effort to reach the data subject(s) affected, then public communication or similar measure should be employed[102].

The controller is liable for any damage caused by a processing that violated the GDPR[103], unless the controller proves that it is not responsible for the cause of the damage[104].

Responsibility of the processor

The processor must be bound by a contract or other legal act under EU or national law with regard to the controller and act in accordance as to the processing operations[105]. Therein 'the subject-matter and duration of processing, the nature and purpose of processing, the type of personal data and categories of data subjects and the obligation and rights of the controller' are set out[106]. Under article 28 para 3 of the GDPR specific clauses to be part of the contract or legal act are foreseen, such as that (a) the processing takes place only under documented instructions by the controller unless the processor is obliged to act so by EU or national law; (b) the processor ensures that authorised persons to process personal data are bound by confidentiality obligation; (c) the processor takes all necessary technical and organisation measures to secure the protection of data subject's personal data; (d) the processor cannot engage other processors unless there is a prior written authorisation of the controller[107] - in case the authorisation is general, the processor has to inform the controller for any intended changes regarding the engaged processors[108]; (d) the processor assist the controller to respond to requests by data subjects exercising their rights under the GDPR; (e) the processor, if requested so by the controller, shall delete or return all personal data to the controller by the end of the provision of services and delete copies unless obliged otherwise by EU or national law; (f) processor provides necessary information to the controller for the latter to establish compliance of the first with the obligation laid down in article 28 GDPR and contribute to audits and inspections conducted by the controller[109]. If, to processor's opinion, a controller's instruction infringes the GDPR, the processor must immediately inform the controller[110]. Standard contractual clauses

98 Art. 33(3).
99 Art. 33(5).
100 Art. 34 paras 1-2.
101 Art. 34(3).
102 Ibid.
103 Art. 82(2).
104 Art. 82(3).
105 Art. 28(3).
106 Ibid.
107 Art. 28(2).
108 Ibid.
109 See also article 28(3), point (f) & article 32: "security of processing".
110 Art. 28(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.

for the aforementioned matters may be laid down by the European Commission or the supervisory authority[111]. In any event, the contract or other legal act must be in writing, including in electronic form[112].

If the processor engages another processor to perform specific processing activities on behalf of the controller, the same data protection obligations must be stipulated in a similar contract or other legal act[113]. Where that processor does not fulfil its data protection obligations, the initial processor remains fully liable to the controller for the acts of the other processor[114]. Sufficient guarantees of implementing appropriate technical and organisational measures in a manner that processing meets the requirements of the GDPR may be demonstrated by the adherence of the processor to an approved code of conduct or certification mechanism[115]. The processor or any person acting under the authority of the controller or the processor, shall process personal data only on the instructions of the controller or the processor, unless EU or national law defines otherwise[116].

Each processor or the representative of a processor in the EU is responsible for keeping a record of all categories of processing operations performed on behalf of the controller, in writing including in electronic form[117]. This record shall be available for the supervisory authority upon request. The same criteria for the obligation to keep record in relation to the size of an enterprise or organisation, as with the controller, apply[118]. In any event, the processor is anticipated to cooperate with the supervisory authority, upon request[119].

The processor as soon as becomes aware of a personal data breach must notify the controller[120].

A processor is liable for damage resulting from a processing only where he has acted contrary to or outside the obligations under the GDPR or the lawful instructions of the controller[121]. The processor is exempted from liability, if it proves that it is not responsible for the cause of the damage[122].

The role of the data protection officer

A data protection officer (DPO) must be designated by the controller or the processor, if: (a) processing is carried out by public authority or body, (b) in the context of the processing, regular and systematic monitoring of data subjects on a large scale takes place, (c) large scale processing of personal data revealing sensitive information about individuals or criminal convictions takes place [123]. Apart from the aforementioned cases, the controller or processor should designate a data protection officer, where required by EU or national law[124]. One data protection officer may serve more controllers or processors[125]. He/she must have expert knowledge of data protection law and practices and the ability to carry out tasks provided under the GDPR[126]. He/she may be a staff member of the controller or processor, or be engaged

111 Art. 28 paras 6-8.
112 Art. 28(9).
113 Art. 28(4).
114 Ibid.
115 Art. 28(5).
116 Art. 29.
117 Art. 30 paras 2& 4.
118 GDPR article 30 para 5.
119 Article 31 GDPR.
120 GDPR Article 33 para 2.
121 GDPR article 82 para 2.
122 GDPR article 82 para 3.
123 GDPR article 37 para 1.
124 GDPR article 37 para 4.
125 GDPR article 37 paras 2-3.
126 GDPR article 37 para 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.

by a service contract[127]. Contact details of the DPO shall be published and communicated to the supervisory authority too.[128]

DPO shall be involved in all issues concerning the protection of personal data[129] and shall directly report to the highest management level of the controller or processor[130]. The controller and processor support the DPO in carrying out his/her tasks under the GDPR (resources, access to personal data processing activities, continuous training)[131] and do not instruct him/her[132]. However, the controller or processor shall make sure that there is no conflict of interest, if the DPO is engaged in several positions[133]. In any event, DPO must be bound by secrecy or confidentiality with regard to his/her tasks[134]. Finally, DPO should be available for data subjects to contact him/her in relation to their personal data[135].

Under article 39 para 1 of the GDPR the DPO is assigned with specific tasks, namely (a) 'to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to' the GDPR and to other EU or national data protection provisions; (b) 'to monitor compliance with' the GDPR, with other EU or national 'data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits'; (c) 'to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35' of the GDPR; (d) to cooperate with the supervisory authority; (e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36' of the GDPR, 'and to consult, where appropriate, with regard to any other matter'.

During the performance of his/her tasks, the DPO has to take into consideration the risks deriving from processing activities, including the nature, scope, context and purposes of processing[136].

2.1.2.5 Data protection safeguards

- *Data protection by design and by default*

By design of the processing and implementation of it, the controller has to apply technical and organisational measures for safeguarding data protection principles effectively[137]. Moreover, by default, the amount of personal data collected, the extent of their processing, the period of storage and their accessibility must be regulated in a manner that all principles are ensured[138].

- *Security of processing*

The controller and processor have to take all necessary technical and organisation measures to ensure data protection and prohibit personal data breaches or any other potential risks for the rights and freedoms of

127 GDPR article 37 para 6.
128 GDPR article 37 para 7.
129 GDPR article 38 para 1.
130 GDPR article 38 para 3.
131 GDPR article 38 para 2.
132 GDPR article 38 para 3.
133 GDPR article 38 para 6.
134 GDPR article 38 para 5.
135 GDPR article 38 para 4.
136 GDPR article 39 para 2.
137 GDPR, article 25, para 1.
138 GDPR, article 25, para 2.

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.

natural persons[139]. Pseudonymisation and encryption are introduced as measures which could be applied to reduce these risks[140]. In the case of pseudonymisation, it is stipulated that additional information which could render a natural person identifiable should be kept separately[141]. Furthermore, to ensure a level of security against such risks, measures that safeguard the ongoing confidentiality, integrity, availability and resilience of processing systems and services, or that restore the availability and access to personal data in a timely manner in the event of a physical or technical incident shall be implemented. Therein, the establishment of a process for regularly testing, assessing and evaluating the effectiveness of the security measures is provided. Additional safeguards can be adherence to an approved code of conduct[142] or an approved certification mechanism[143]. At any event, in assessing the security level, risks to be considered should be the ones deriving 'from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed' [144]. Moreover, precautions must be taken for natural persons acting under the authority of the controller or the processor who have access to personal data to process them only on instructions from the controller or according to EU or national law[145].

- *Codes of conduct*

Codes of conduct are encouraged to be drafted to contribute to the proper application of the GDPR by the Member States, the supervisory authorities[146], the European Data Protection Board[147] and the European Commission[148]. 'Associations and other bodies representing categories of controllers or processors may prepare codes of conduct or amend or extend such codes' to specify the application of the GDPR, with regard to the particular features of the processing operation and principles for data protection and processing (e.g. fair and transparent processing, legitimate interest of the controller, collection of personal data, pseudonymisation, information provision to data subjects)[149]. The monitoring of compliance with a code of conduct, as foreseen in article 41 GDPR, 'may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

- *Processing which does not require identification*

In case the controller is not able to identify a data subject from the personal data processed, then the controller should not be obliged to obtain additional information in order to identify the data subject, unless this is offered by the data subject in order to help the latter exercise his/her rights. In such a case, an authentication mechanism could be applied as a digital identification of the data subject (e.g. logging in to the online service)[150].

- *Data protection impact assessment and prior consultation*

[139] See for example recital 28 GDPR; articles 25 & 32 GDPR.
[140] Article 32 para 1 & recital 28 GDPR.
[141] Ibid.
[142] See article 40 GDPR.
[143] See article 42 GDPR.
[144] GDPR, article 32 para 2.
[145] GDPR, article 32 para 4.
[146] See articles 51-59 GDPR.
[147] See articles 68-76 GDPR.
[148] GDPR, article 40, para 1.
[149] GDPR, article 40 para 2.
[150] Recital 57 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.

When there is the likelihood that a type of processing, particularly by the use of new technologies, could result in a high risk to the rights of natural persons, the controller should conduct beforehand an assessment of the impact of the intended processing operations on the protection of personal data[151]. This would be particularly required in case of (a) systematic and extensive evaluation of personal aspects of natural persons, based on automated processing, including profiling, and which further becomes grounds for decisions that produce legal effects for the natural person or significantly affect him/her, (b) processing on a large scale of special categories of data revealing sensitive information about a natural person[152], or of personal data relating to criminal convictions and offences[153]; (c) a systematic monitoring of a publicly accessible area on a large scale[154]. Similar processing operations that present the same high risk could be addressed with one single assessment[155]. Such processing occasions should be listed by the supervisory authority, as well as those cases where no impact assessment is necessary[156]. Where processing is based on EU or Members State law under specific clauses[157] to which the controller is subject, a data protection impact assessment has already been carried out in the context of the adoption of that legal basis[158].

Under article 35 para 7 of the GDPR, the minimum content of an assessment is provided. In accordance, the assessment should contain at least: (a) a systematic description of the anticipated processing operations and its purposes, including, where applicable, the legitimate interest pursued by the controller, (b) an assessment of the necessity and proportionality of the processing in relation to the purposes, (c) an assessment of the risks to the rights and freedoms of data subjects, and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned. Compliance with approved codes of conduct will be taken into account for the assessment[159].

Where a data protection impact assessment indicates that the processing would result in a high risk, if no measures are taken by the controller to mitigate the risk, the controller must consult the supervisory authority prior to processing[160].

2.1.2.6 Data subject's rights

GDPR provides for the rights of the data subject in relation to the processing of his/her personal data. The controller should facilitate the exercise of the data subject's rights by providing modalities, such as easily accessible and free of charge mechanisms to make the request[161].

Right to be Informed

- *Information to be provided, where personal data have been collected from the data subject*

As soon as personal data are obtained from the data subject and insofar as the data subject is not already aware of, the controller has to provide certain pieces of information, such as (a) the identity and contact

[151] GDPR, article 35, para 1.
[152] See also article 9(1) GDPR.
[153] See also article 10 GDPR.
[154] GDPR, article 35, para 7.
[155] GDPR, article 35, para 1.
[156] GDPR, article 35, paras 4-5.
[157] See GDPR, article 6 para 1, point (c) or (e).
[158] GDPR, article 35 para 10.
[159] GDPR, article 35, para 8.
[160] See article 36 GDPR.
[161] See recital 59 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.

details of the controller or the controller's representative[162], (b) the contact details of the data protection officer where applicable, (c) the purpose of the personal data processing and the legal basis for it, (d) if processing is based on the legitimate interest of the controller, then these should be made known (e) the recipients of the personal data, if any (f) where applicable, the intention to transfer of data[163]. Apart from the aforementioned, the controller shall provide further information about (a) the time period of data storage, (b) the existence of the right to request access to and rectification or erasure of personal data or restriction of processing, as regards the data subject's personal data or to object to processing as well as the right to data portability, (c) when processing is based on the data subject's consent, the right to withdraw consent at any time, without affecting the lawfulness of processing before its withdrawal, (d) the right to lodge a complaint with a supervisory authority, (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of not providing them, (f) the existence of automated decision-making, including profiling, the logic involved and the significance or potential consequences of such processing for the data subject[164]. Lastly, if the controller intends to proceed with further processing of the data subject's personal data for a purpose different from the one for which the data where initially collected, then the data subject must receive all relevant information[165].

- *Information to be provided, where personal data have not been collected from the data subject*

In case the personal data have not been obtained from the data subject and the latter is not already aware of, the controller has the same obligation to inform the data subject within a reasonable period after obtaining the personal data, but at least within a month or if applicable in the first communication with the data subject or if applicable in the first disclosure of the data to another recipient[166]. In addition to the previously mentioned, the controller has to further inform the data subject about the categories of personal data concerned[167] and the sources from which the data originate and whether these publicly accessible sources[168]. Information should be provided free of charge[169]. These is no obligation for the controller to inform the data subject, if this proves impossible or involves disproportionate effort or it might not serve the objectives of the processing[170]. Making information publicly available could balance both sides interests[171]. Moreover, where obtaining or disclosure is directly provided in EU or national law taking into account the necessary rights protection safeguards or where data must remain confidential (statutory obligation of secrecy), the controller shall not provide any information to the data subject[172].

Right of access by the data subject[173]

[162] 'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation; Article 4 (17) GDPR.
[163] Article 13 (1), (4) GDPR.
[164] Article 13(2) GDPR.
[165] Article 13(3) GDPR.
[166] Article 14 (1)-(4) GDPR.
[167] Article 14(1), point (d) GDPR.
[168] Article 14(2), point (f) GDPR.
[169] Article 12(5) GDPR.
[170] Article 14(5), point (b) GDPR.
[171] In this case the legislator suggests that appropriate measures should be taken to protect the data subject's rights and interests, including making the information publically available; Article 14(5)b GDPR.
[172] Article 14(5), points (c)-(d) GDPR.
[173] Article 15 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.

The data subject holds the right to receive a confirmation as to whether or not his/her personal data are being processed and where that is the case to information such as the purpose of processing, the categories of personal data in question, the recipients that the data have been or will be disclosed, the existence of the right of rectification or erasure of personal data or restriction of processing or the right to object to the processing, the right to lodge a complaint; the sources from which the controller collected the data, the existences of automated decision-making. Moreover, the controller shall provide a copy of the personal data being processed[174]. Importantly, the controller should verify the identity of a data subject prior to giving access[175].

Right to rectification[176]

The data subject has the right to demand from the controller to correct inaccurate personal data. If data are incomplete, the data subject has the right to have them completed.

Right to erasure ('right to be forgotten')[177]

Under certain conditions, the data subject has the right to demand from the controller the erasure of personal data without undue delay. These conditions are limited to the following[178]:

(a) the necessity principle is no longer satisfied in relation to the purposes for which the personal data were initially collected or processed;
(b) where consent was the only legal basis for personal data processing and the data subject withdraws consent;
(c) the data subject objects to the processing in the context of controller's task performance in the public interest or on controller's legitimate interests and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing for marketing purposes;
(d) the personal data have been unlawfully processed;
(e) the personal data have to be erased for compliance with a legal obligation in EU or national law to which the controller is subject;
(f) the personal data have been collected from a person below 18 years of age in the context of information society services[179].

In case of personal data made public by the controller and the latter is obliged to erase the personal data, the controller has to take all reasonable measures to inform controllers processing these personal data too, that the data subject has requested erasure 'of any links to or copy or replication of those personal data'[180].

However, the right to erasure is balanced with other rights, legal obligations or reasons and, to the extent that processing is necessary for respecting these, can only partly apply[181]. Such cases are the right to freedom of expression and information, the legal obligation to comply with EU or national law or the

[174] See also Recital 63 GDPR.
[175] Recital 64 GDPR.
[176] Article 16 GDPR.
[177] Article 17 GDPR.
[178] GDPR, article 1, para 1.
[179] For example, if a person had given his/her consent as a child and was not aware of the risks deriving from the processing, and later on, as an adult, desires to remove his/her personal data especially from the internet; recital 65 GDPR.
[180] GDPR, article 17, para 2.
[181] GDPR, article 17, para 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.

exercise of official authority of the performance of a task in the public interest where in all previous occasions processing is required, the public interest for public-health related reasons, archiving purposes in the public interest, 'scientific or historical research purposes or statistical purposes in accordance with Article 89(1)' GDPR 'in so far as reassure of personal data is likely to render impossible or seriously impair the achievement of the objectives of that processing' and the right to exercise and defend a legal claim[182].

Right to restriction of processing

In terms of provisional protection, the data subject has the right to obtain from the controller restriction of processing[183] under specific circumstances, which are: when the accuracy of personal data is contested by the data subject (for necessary time to the controller to verify the accuracy); the processing is unlawful and the data subject's requests restriction of processing and not erasure of the personal data; the personal data are no longer necessary for the purposes of processing, but the data subject needs them to establish, exercise or defend legal claims; the data subject has objected to the legitimate interests of the controller and claims are examined[184]. In these cases, personal data cannot be processed unless with the data subject's consent or for the purpose of establishing, exercising or defending legal claims or for protecting the rights of another natural or legal person of for reasons of important public interest of the EU or of a Member State[185]. If restriction is about to be lifted, the controller must inform the data subject beforehand[186].

Right to data portability

Where processing of personal data is based on the data subject's consent and this is conducted through automated means, the data subject has the right to receive his/her personal data from the controller who was provide with the data, 'in a structured, commonly used and machine-readable format' and transmit those data to another controller[187]. This right does not apply 'to processing necessary for the performance of task carried out in the public interest or in the exercise of official authority vested in the controller'[188] or when it significantly impacts the rights and freedoms of others[189].

Right to object

Under certain conditions, the data subject has the right to object at any time to the processing of his/her personal data, which was grounded on the performance of tasks in the public interest or on the legitimate interests of the controller[190]. Unless the controller demonstrates that there are interests overriding the data subject's rights or that processing is necessary for the exercise of legal claims, the controller shall no longer process the personal data[191]. Until the first communication with the data subject, the controller must inform the data subject about this right explicitly[192]. Furthermore, 'where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to

[182] See also recital 67 GDPR
[183] See also recital 67 GDPR
[184] GDPR, article 18, para 1.
[185] GDPR, article 18, para 2.
[186] GDPR, article 18, para 3.
[187] GDPR, article 20, para 1. See also Recital 68 GDPR.
[188] GDPR, article 20, para 3.
[189] GDPR, article 20, para 4.
[190] GDPR, article 21, para 1.
[191] Ibid. Paras 2 & 3 concern processing for marketing purposes, which the data subject unconditionally can object to (see also recital 70 GDPR).
[192] GDPR, article 21, para 4.

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 of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest'[193].

Right not to be subject to a decision based solely on automated processing

The data subject has the right not to be subjected to a decision which is based on the evaluation of personal aspects that have been automatically processed, namely profiling, and which has legal effects upon him/her or significantly affects him/her[194]. The right is not applicable in case such a decision is (a) necessary for entering into, or the performance of a contract between the controller and the data subject, (b) is authorised by EU or national law and the controller adheres to it (e.g. fraud and tax-evasion monitoring) and which foresees appropriate safeguards for the data subject's rights, (c) is based on the data subject's explicit consent[195]. Under (a) and (c) occasions, the controller has to provide suitable measures to ensure the data subject's rights and interest, such as 'the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision'[196]. Such measure cannot involve a child data subject[197].

- The controller must provide information on action taken upon the request of the data subject under articles 15-22 of the GDPR without undue delay and in any event within one month from the receipt of the request[198].

Restrictions

Restrictions to the rights of the data subject and corresponding obligations of the controller may be imposed by EU or national law, as long as these respect fundamental rights and freedoms and is a necessary and proportionate measure to safeguard: national security; defence; pubic security; operations related to criminal offences or the execution of criminal penalties; other significant objectives of public interest of the EU or of a Member State; the protection of judicial independence and judicial proceedings; the prevention/investigation/detection/prosecution of breaches of ethics for regulated professions; monitoring, inspection or regulatory function related to the exercise of official authority; the protection of rights and freedoms of the data subject or others; the enforcement if civil law claims (GDPR, article 23, para 1). Such legislative measure shall contain minimum specific provision as stipulated under para 2 of the article 23 GDPR.

Right to remedy

Every data subject has the right to lodge a complaint before the competent supervisory authority[199]. In case the supervisory authority does not handle the complaint or does not inform the subject within three months on the progress or outcome of the complaint, the data subject has the right to an effective judicial remedy[200]. Furthermore, every natural or legal person has the right to an effective judicial remedy against a legally binding decision of a supervisory authority that concerns them[201]. The data subject, who considers that his/her rights under the GDPR have been violated by the controller due to processing in non-

[193] GDPR, article 21, para 6.
[194] GDPR, article 22, para 1.
[195] GDPR, article 22, para 2. See also recital 71 GDPR.
[196] GDPR, article 22, para 3.
[197] Recital 71, GDPR.
[198] The time period may be extended if necessary and the controller has to inform the data subject for any extension; GDPR, article 12 para 3.
[199] Article 77 GDPR.
[200] GDPR, article 78, para 2.
[201] GDPR, article 78, para 2.

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.

compliance with the GDPR, has, in addition, the right to an effective judicial remedy (directly)[202]. In case controllers were two or more, the data subject may exercise his/her rights under the GDPR against each of the controllers[203]. If such an infringement of the GDPR has caused material or non-material damages to a person, then the controller or the processor have to compensate the person[204].

2.2 National Legislation

SPHINX ecosystem will be evaluated in 3 pilots located in Greece, Portugal and Romania. The following section provides an overview of national legislation concerning personal data administration in each country.

2.2.1 Greece

2.2.1.1 The right to private life and the protection of personal data under the Greek Constitution

The right to private life

Under article 9(1) of the Greek Constitution, "the private and family life of an individual is inviolable". As a significant aspect of the free development of personality, the right to private life is expressly stipulated in the 1975 Constitution, influenced by the provisions of Article 8 of the 1951 European Convention on Human Rights on the right to respect of a person's private and family life, home and correspondence[205]. The right to private life constitutes a right with evolving concept and scope. In order to meet current protection safeguards, in light of technological advancements in the sector of information and communication, as well as of the intrusion of the mass media and the internet into a person's private sphere, an evolving interpretation is deemed necessary. In the context of article 9(1) of the Constitution, the individual is protected against intrusion from others, public authorities or other natural and legal persons.

The right holders are natural persons, nationals and non-nationals and under conditions persons under the 18 years of age.

Main infringements of the right to private life can be a) the disclosure of an individual's personal data related to his/her private sphere without his/her consent or with no legal and justified grounds in the public interest, b) the surveillance with the use of technology and devices, which can result in the disclosure of data containing sensitive information and place a risk to the individual's fundamental rights and freedoms, and c) transmission of information related to an individual's private life[206].

The right to private life is connected with articles 9 A of the Constitution on the right to the protection of personal data and article 19(1) on the right to communications confidentiality and thus must be examined in conjunction. All the aforementioned comprise the principal aspects of an individual's private sphere, especially with regard to communication and exchange and transmission of information and data.

[202] Article 79 GDPR.
[203] GDPR, Article 26 para 3.
[204] Article 83 GDPR.
[205] See also Ακριβοπούλου Χ.Μ., Άρθρο 9, in: Σύνταγμα, Κατ' άρθρο ερμηνεία, Φ. Σπυρόπουλος, Ξ. Κοντιάδης, Χ. Ανθόπουλος, Γ. Γεραπετρίτης (eds), Εκδόσεις Σάκκουλα, Αθήνα- Θεσσαλονίκη, 2017.
[206] Δαγτόγλου Π. Δ., Συνταγματικό δίκαιο, Ατομικά δικαιώματα, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη, 2012, p. 331.

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 right to the protection of personal data

In article 9 A of the Greek Constitution it is stipulated that 'All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law. The protection of personal data is ensured by an independent authority, which is constituted and operates as specified by law'. This clause has been introduced with the 2001 revision of the Constitution in alignment with European standards. Within the scope of this provision falls every information which relates to an identified or identifiable natural person in the context of both his/her private sphere and in the public sphere[207,208]. In addition, it includes all aspects of intervention and not solely automated processing, though the risks of technological developments are considered. Limitation to the right can be imposed only where provided by law setting requirements such as the informed consent of the data subject or the exercise of other rights (e.g. to information, to freedom of expression, to a legal claim) or a public interest (e.g. the investigation of crimes)[209]. In any event, the principle of proportionality, as stipulated in article 25 of the Constitution, must be met and the respect and protection of the value of the human being should be guaranteed[210,211].

The right to personal data protection concerns every natural person. Legal persons' data are not personal data. Under the constitutional provision, state authorities, bodies and agencies shall ensure the unhindered implementation of the right and for this shall take also safeguard measures[212]. Furthermore, an independent authority must be in place to ensure the implementation of the right to personal data protection.

The right to confidentiality of correspondence

According to article 19(1) of the Constitution, 'secrecy of letters and all other forms of free correspondence or communication shall be absolutely inviolable. The guaranties under which the judicial authority shall not be bound by this secrecy for reasons of national security or for the purpose of investigating especially serious crimes, shall be specified by law'. Though the article was stipulated in the 2001 Constitution's revision, within the meaning of correspondence, all current means of communication are included. This constitutional protection is provided for communications where the individual (a party) expresses a reasonable subjective expectation that the content and other elements of the communication will not be disclosed to third parties[213]. Data identified and protected in the course of communication comprise of the content of the messages transmitted, the data necessary for the establishment and maintenance of a communication (communication partners, time and duration of the communication; traffic data) and the data related to the location of the communication device employed (location data)[214]. Limitations to the

[207] See Council of State, Decision 1616/2012.

[208] Μίτλεττον Φ., Η έννοια των προσωπικών δεδομένων, in: Προσωπικά δεδομένα, Κοτσαλής Λ. (ed.), Νομική Βιβλιοθήκη, 2016, Νομική Βιβλιοθήκη, 2016, p. 10.

[209] Μήτρου Λ., Άρθρο 9 Α, in: Σύνταγμα, Κατ' άρθρο ερμηνεία, Φ. Σπυρόπουλος, Ξ. Κοντιάδης, Χ. Ανθόπουλος, Γ. Γεραπετρίτης (eds.), Εκδόσεις Σάκκουλα, Αθήνα- Θεσσαλονίκη, 2017, p. 225.

[210] Article 2(1) of the Constitution.

[211] See Council of State, Decision 3545/2002.

[212] Μίτλεττον Φ., Η έννοια των προσωπικών δεδομένων, in: Προσωπικά δεδομένα, Κοτσαλής Λ. (ed.), Νομική Βιβλιοθήκη, 2016, Νομική Βιβλιοθήκη, 2016.

[213] Παπαδόπουλος Ν., Άρθρο 19, in: Σύνταγμα, Κατ' άρθρο ερμηνεία, Φ. Σπυρόπουλος, Ξ. Κοντιάδης, Χ. Ανθόπουλος, Γ. Γεραπετρίτης (eds.), Εκδόσεις Σάκκουλα, Αθήνα- Θεσσαλονίκη, 2017, p. 477 citing ECHR case law.

[214] Παπαδόπουλος Ν., Άρθρο 19, in: Σύνταγμα, Κατ' άρθρο ερμηνεία, Φ. Σπυρόπουλος, Ξ. Κοντιάδης, Χ. Ανθόπουλος, Γ. Γεραπετρίτης (eds.), Εκδόσεις Σάκκουλα, Αθήνα- Θεσσαλονίκη, 2017.

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.

right to confidentiality may be introduced in case (a) it is necessary for complying with a legal provision; (b) safeguards are in place that prohibit any infringement of the constitutional statutes; (c) there is court order to do so; (d) this serves the purposes of public security and the investigation of serious crimes[215].

2.2.1.2 Legal framework on personal data protection and processing

2.2.1.2.1 Main provisions

The principal legal instrument regulating the protection of personal data was up until May 2018 law 2472/1997 as amended[216], which was originally adopted to transpose the 'Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data' into national law. However, from 25 May 2018 and on, the General Data Protection Regulation came into force directly in all Members States. Therefore, law 2472/1997 was repealed. For the necessary changes and adjustments in national legislation, law 4624/29-08-2019 was adopted[217]. The new law includes regulatory measures for the correct implementation of the GDPR nationwide and the transposition of the Police Directive into national law. Therefore, the law provides in Greek and within the Greek context all principles, measures, safeguards, processes, rules, exceptions and rights which are included in the GDPR and the Police Directive. A more concrete provision on making certain personal data public where a crime is being investigated is also foreseen. In addition, the upcoming role of the independent supervisory authority is laid down.

2.2.1.2.2 The role of the Authority for the Protection of Personal Data

The role of the national supervisory authority, "the Authority for the Protection of Personal Data"[218], has changed by the introduction of the GDPR. To this end, no particular prior permission from the competent independent authority is necessary for the processing of personal data. To the contrary, the Regulation has established a certain procedure and safeguard measures to be applied in order for every controller and processor to know beforehand how compliance directly with the GDPR can be achieved. At the same time, the national supervisory authorities may set forth more concrete rules for processing activities that involve various categories of personal data and monitor the implementation of the GDPR in the country by providing consultation, conducting investigation, receiving complaints and issuing decisions. In the context of an investigation the member of the national authority has the right to have full access to the processing operations except for public security cases or for serious crime investigation[219].

All members of the Greek Authority for the Protection of Personal Data are bound by a duty of confidentiality. In case of any personal data leak by a member of the authority, the perpetrator is charged with fine or even incarceration and violations are regarded as cause of disciplinary action too. The national independent authority, pursuant to the provisions under articles 57 & 58 of the GDPR should, inter alia, encourage the drawing up of codes of conduct[220] and provide an opinion and approve such codes of

[215] Δαγτόγλου Π. Δ., Συνταγματικό δίκαιο, Ατομικά δικαιώματα, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη, 2012, σελ. 361.

[216] Consolidated version of the law, available at: http://www.dpa.gr/pls/portal/url/ITEM/E3BC3C1B7FC83BA6E040A8C07D24022A

[217] https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/nomos-4624-2019-phek-137a-29-8-2019.html

[218] Website of the Greek Authority for the Protection of Personal Data available at: http://www.dpa.gr/portal/page?_pageid=33,15048&_dad=portal&_schema=PORTAL

[219] Draft available at: http://www.opengov.gr/ministryofjustice/wp- content/uploads/downloads/2018/02/sxedio_nomou_prostasia_pd.pdf

[220] See article 40(1) 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.

conduct [221]; encourage the establishment of data protection certification mechanisms and of data protection seals and marks[222] and approve the criteria of certification[223].

2.2.1.3 Legal framework in electronic communications privacy

2.2.1.3.1 Main provisions and the case of disclosing communication

The primary legal instrument regulating privacy issues in the electronic communications sector is the law 3471/2006 which transposed the E-privacy Directive (2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector) into national law. Within the scope of the law falls any type of communication through land and mobile telephony, as well as the internet (public communications services & networks). Further on, by law 3674/2008 more safeguard measures were introduced such as obligations of the communication service providers to draft security policies, to encrypt voice messages, to record any processing activity, to inform the user and the supervisory authority where a personal data breach has occurred[224]. As the 2002 e-privacy directive was significantly amended by the Directive 2009/136/EC, law 3471/2006 had to be amended accordingly. Therefore, with the law 4070/2012 under articles 168-173 modifications were introduced to law 3471/2006[225].

The meaning of personal data breach has been broadened pursuant to the provisions of the amended e-privacy Directive, as new forms of breach were discovered[226]; 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service. In accordance, the obligations of the service provider where a data breach has occurred were more explicitly laid down pursuant to article 4(3) of the E-privacy Directive[227].

With regard to the security of processing and without prejudice to the principal legal instrument on data protection (be it previously the Directive 95/46/EC and now the GDPR), the service providers must ensure that personal data can be accessed only by authorised personnel; protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure; and ensure the implementation of a security policy with respect to the processing of personal data[228].

Provisions on traffic data and location data, as previously analysed, cover not only the new forms of services provided through land and mobile telephony, but also the services provided by social networking sites[229]. Processing of location data is prohibited unless the user has provided his/her consent (which can withdraw at any time) or the competent authorities for emergency situations or law-enforcement and

[221] See article 40(5) GDPR.

[222] See article 42(1) GDPR.

[223] See article 42(5) GDPR.

[224] Available at: http://www.adae.gr/fileadmin/docs/nomoi/N.3674.2008.pdf

[225] Consolidated version of the law 3471/2006, available at: http://www.dpa.gr/pls/portal/url/ITEM/DEF1C46F2229C66FE040A8C07C246917

[226] Article 2(11) Law 3471/2006.

[227] Article 12(2) Law 3471/2006.

[228] Article 12(3), law 3471/2006.

[229] Μίτλεττον Φ., Η έννοια των προσωπικών δεδομένων, in: Προσωπικά δεδομένα, Κοτσαλής Λ. (ed.), Νομική Βιβλιοθήκη, 2016, Νομική Βιβλιοθήκη, 2016.

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.

judicial authorities, first aid services and fire-brigade request the location data to identify the call and further to manage an emergency or investigating a crime[230].

Confidentiality of communications may be restricted only in compliance with the Constitution. Law 2225/1994 regulates the lifting of confidentiality according to the constitutional statute for the purposes of either public security or the investigation of serious crimes[231]. In the latter case, lifting of confidentiality can be ordered by the Judicial Council after a request from the Public Prosecutor or the Investigating Magistrate. Within 24 hours, the Council must issue a decision. In exceptional cases, the Public Prosecutor or the Investigating Magistrate can order the lifting of confidentiality and within 3 days, they have to introduce the request before the competent Judicial Council. Additional safeguard action has to be taken for the prevention of abusing such measures. Consequently, for each order for lifting confidentiality the Authority for Communication Security and Privacy, the competent Minister (of Justice) and to the body in charge (management committee/ council/ board) of the legal person of the communication service provider or network must be notified. Moreover, the competent judicial authority shall write a report for each order issued concerning the lifting of confidentiality; the measure has to be limited to the minimum necessary duration and the user (data subject) holds the right to be notified after the measure has been taken.

2.2.1.3.2 The role of the Authority for Communication Security and Privacy

The national independent authority for safeguarding the privacy of communications, the "Authority for Communication Security and Privacy"[232], was established with Law 3115/2003 (article 1)[233], pursuant to article 19(2) of the Greek Constitution. The authority is, inter alia, responsible for monitoring the cases were lifting of confidentiality has been employed; carries out investigations; receives complaints; keeps a record of personal data processing and provides advices on issues of privacy. According to the amended article 6(4) of Law 3471/2006, the national authority issues acts where the procedure, the means and any other technical detail for disclosing location data is described.

2.2.2 Portugal

2.2.2.1 The right to private life and the protection of personal data under the Portuguese Constitution

According to Article 26[234] of the Constitution of the Portuguese Republic, to all citizens are recognised the rights to personal identity, personality development, civil capacity, citizenship, good name and reputation, image, word, privacy and private protection of privacy and legal protection against any forms of discrimination

---

[230] Article 6(4) & (5) Law 3471/2006 as amended.

[231] Lifting of Confidentiality is permissible for the investigation of felonies under:
(a) articles 134, 135(1)&(2), 135 A, 137 A, 137 B, 138, 139, 140, 143, 144, 146, 148(2), 150, 151, 157(1), 168(1), 187(1)&(2), 207, 208(1), 264 points (b)&(c), 270, 272, 275 point (b), 291(1) point (b)&(c), 229, 322, 324(2)&(3), 374, 380, 385 of the Penal Code; Article 4(1) point (a) of law 2225/1994 as amended by Law 3658/2008. Kidnapping for the purpose of ransom or kidnapping of a child under 14 years old falls under this provision.

[232] Website of the Hellenic Authority for Communication Security and Privacy available at: http://www.adae.gr . Relevant legislation available at: http://www.adae.gr/nomothetiko-plaisio/elliniki-nomothesia/nomoi-gia-to-aporrito-epikoinonion/

[233] Available at: http://www.adae.gr/fileadmin/docs/nomoi/N.3115-2003.pdf

[234] https://dre.pt/web/guest/legislacao-consolidada/-/lc/337/201905280100/diploma/2?rp=diploma&q=Constituição+da+República+Portuguesa&did=34520775&filter=Filter

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 provided in the same article that the law approved by the Assembly of the Republic will establish the effective guarantees against obtaining and using information relating to individuals and families in ways that are abusive or contrary to human dignity.

Article 35 of the Constitution of the Portuguese Republic also provides that all citizens have the right to access computerised data concerning them, which may require rectification and updating, and the right to know the purpose for which that data are intended, in accordance with law.

The same article also stipulates that the law defines the concept of personal data as well as the conditions applicable to its automated processing, connection, transmission and use, and ensures its protection, in particular through an independent administrative entity.

It is expressly provided in the aforementioned article that information technology cannot be used for the processing of data concerning philosophical or political beliefs, party or trade union affiliation, religious faith, private life and ethnic origin, except with the explicit consent of the holder. Article 35 also prohibits access to personal data of third parties, except in exceptional cases provided for by law, as well as the granting a single national number to citizens.

The same article provides for free access to computer networks for public use, with the law defining the regime applicable to cross-border data flows and appropriate forms of protection of personal and other data which safeguard is justified on grounds of national interest.

Finally, that article stipulates that the personal data contained in manual files enjoy the same protection as provided for in the preceding paragraphs, in accordance with the law.

2.2.2.2 Legal framework on personal data protection and processing

2.2.2.2.1 Main provisions

Regulation no. 798/2018[235] - published in the Diário da República (Official State Gazette) at the Portuguese Independent Supervisory Authority – CNPD request which makes public in its Regulation No. 1/2018[236] the list of treatments of personal data subject to a Data Protection Impact Assessment (DPIA) because they are susceptible to involve a high risk to the rights and freedoms of natural persons have to be preceded by an DPIA. The European legislator defines, by way of example, three types of situations which fulfil the requirements of this obligation of the data controller and which are embodied in Article 35 (3) of the RGPD. In addition to these, the CNPD in its Regulation 1/2018 lists other treatments likely to imply that risk, thus corresponding to the list that now presents itself to treatments that also fulfil the assumptions of paragraph 1 of article 35., and with reference to the DPIA and determining whether the treatment is 'likely to result in a high risk' for the purposes of Regulation (EU) 2016/679 - WP248 rev.01 pp. 10-12, adopted by the Article 29 Working Party and adopted by the European Data Protection Committee.

- Law 67/98[237], of October 26, this law remains in force in everything that does not contravene the Regulation (EU) No. 2016/679, that are detailed in section 2.2.3.4 – The enforcement of the GDPR in Portugal.

235 https://dre.pt/home/-/dre/117182365/details/maximized

236 https://www.cnpd.pt/bin/decisoes/regulamentos/regulamento_1_2018.pdf

237 https://dre.pt/web/guest/pesquisa/-/search/239857/details/maximized?p_p_auth=i8kXyLU6

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.

- Regulation (EU) No. 2016/679 of 27 April 2016[238] - Protection of individuals with regard to the processing of personal data and on the free movement of such data.

- Resolution of the Council of Ministers No. 41/2018[239] - establishes the minimum procedures and technical requirements of the networks and information systems regarding the organisation security that are required or recommended to all services and entities of the State's direct and indirect Administration. This resolution aims to prepare the Portuguese Public Administration to comply with the concept of privacy by design and by default as stated in article 35 of GDPR, which requires organisations to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights.

2.2.2.2.2 The role of the Authority for the Protection of Personal Data

- Regulation (EU) No. 2016/679 of 27 April 2016, articles 51.º and 52.º - supervision of compliance with the General Regulation for the Protection of Personal Data.

The supervisory authorities act in complete independence in the performance of their duties and in the powers conferred on it under the Regulation.

2.2.2.3 Legal Framework in electronic communications privacy

2.2.2.3.1 Main provisions and the case of disclosing communications

Law nº 41/2004, amended and republished by Law nº 46/2012, of August 29[240] - Regulates the protection of personal data in the electronic communications sector, transposing to the legal system the Directive 2002/58/EC of the European Parliament and of the Council of 12 July on the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Article 2 of Directive 2009/136/EC of the European Parliament and of the Council of November.

Regulation (EU) No. 611/2013[241] - Measures applicable to the notification of breaches of personal data in accordance with Directive 2002/58 / EC of the European Parliament and of the Council on privacy and electronic communications

2.2.2.3.2 The role of the Authority for Communication Security and Privacy

According to the Law 41/2004, amended and republished by Law n.º 46/2012, of August 29, the Authorities have the following roles:

- draw up regulations concerning practices to be adopted to comply with this law;

- give orders and make recommendations;

- publish codes of conduct;

- publish other information deemed relevant;

- prosecution, investigation and filing of cases of misconduct, as well as the application of admonitions, fines and sanctions accessory

238 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

239 https://dre.pt/home/-/dre/114937034/details/maximized

240 https://dre.pt/pesquisa/-/search/174793/details/maximized

241 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R0611

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.

2.2.2.4 The enforcement of the GDPR in Portugal

In order to contribute to the implementation of an area of freedom, security, justice and economic union, economic and social progress, the consolidation and convergence of economies in the internal market and the well-being of natural persons the European Union (EU) adopted the General Regulation on Data Protection (EU) 2016/679 (RGPD) which revoked the previous Directive 95/46/EC.

The objectives and principles of Directive 95/46 are still valid, but did not avoid the fragmentation of the application of data protection at Union level or the feeling that there are still significant risks for the protection of natural persons, in particular regarding electronic activities, seeing how differences in the level of protection of rights and natural persons may obstruct the free movement of personal data within the Union. These differences between the various levels of protection are caused by disparities in the implementation and application of Directive 95/46/EC.

As of May 25, 2018, the GDPR has been fully applied throughout the European Union and, therefore, also in Portugal making necessary the approval of national legislation that complements the GDPR, which to this day has not yet happened.

Therefore, until national legislation complementing the GDPR has been approved, and which revokes Law 67/98[242], of October 26, this law shall remain in force in everything that does not contravene that European diploma.

Accordingly, the CNPD, as an independent administrative entity with powers of authority and with the task of guaranteeing fundamental rights in the processing of personal data, has the powers conferred by Portuguese Law 67/98, and other special legislation, in relation to treatments of personal data relating to crime prevention, investigation and prosecution.

In the context of the application of the regulation, still within the scope of Law 67/98, the CNPD understands that there are a number of issues that have changed, of which the following stand out:

1. No longer required to send the prior notification of personal data processing to CNPD, this disappears with the application of the GDPR. It is no longer necessary to request authorisation from the CNPD to carry out processing of personal data covered by the GDPR;
2. A reinforcement in the analysis of treatments based on consent: This will have to be explicit, that is, the person has to express his/her will to authorise. It must also provide the information referred to in Article 13 of the GDPR, appropriate to its specific case, must not forget to inform the owner of the data that it can revoke their consent at any moment and indicating the means by which it can do so.

Finally, until there is national legislation to implement the GDPR that revokes Law 67/98 on subjects covered by the regulation, the Law 67/98 remains in force in everything that does not contradict the GDPR.

2.2.3 Romania

2.2.3.1 The right to private life and the protection of personal data under the Romanian Constitution

Protecting data and information is a priority for the Romanian Government, therefore several Romanian laws state about this matter.

[242] https://dre.pt/web/guest/pesquisa/-/search/239857/details/maximized?p_p_auth=i8kXyLU6

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.

First of all, The Romanian Constitution states in Article 26 that public authorities shall respect and protect intimacy, family and private life. The personal data are processed legally, and are collected for specific, explicit and legitimate purposes and not subsequently processed in an incompatible way with these purposes. The protection of private life is the protection of all information about citizens and their personal life.

The article also recognises fundamental rights for the data subject, such as the right to be informed about what information is being collected and for what purpose, the right to access those data, the right to oppose at any time to the processing, provided that the person has legitimate reasons in this sense. Furthermore, the data subject has the right to oppose to the processing of its personal data, if the purposes of the processing are directed towards marketing research, to obtain or to transmit commercial, advertising or marketing information. This is a right meant to protect the subject and allows him to choose whether he accepts the protection of the law or not. His acceptation signature allows other people or entities to process his personal data.

Article 26 also prohibits access to personal data of third parties, except for exceptional cases provided for by law. According to the Law no. 190/2018 the personal data can be stored for longer periods if they will be processed exclusively for archiving purposes in the public interest, for scientific research or historical purposes.

2.2.3.2 Legal framework on personal data protection and processing

Main provisions

The principal legal instrument regulating the protection of personal data was until July 2018, Law no. 102 adopted on May 3, 2005 regarding the establishment, organisation and functioning of the National Supervisory Authority of Personal Data Processing.

In June 2018, Law no. 129 /2018 was issued for amending and completing Law no. 102/2005 regarding the establishment, organisation and functioning of the National Supervisory Authority for Processing Personal Data. However, from 25 May 2018 and on, the General Data Protection Regulation came into force and applies directly in all Members States.

Therefore, the protection of data was supported by the Law no. 190 of July 18, 2018 on measures to implement the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on protection of natural persons regarding the processing of personal data and regarding free movement of these data by repealing Directive 95/46/ EC (General Regulation regarding data protection).

Law no.190/2018 states general information about data protection with general definitions of used terms, but for medical business it states some special procedures, because medical services work with sensitive information (physical and mental health information) about data subjects. This legislation states that personal information data can be used in medical services only if data subject express his/her consent in written after all explanations needed was given and acknowledged.

The role of the Authority for the Protection of Personal Data

The National Authority for the Supervision of Personal Data Processing was set up through the Law no. 102/2005, which came into force at 12th May 2005. The Authority has the goal of protecting the fundamental rights and freedoms of the natural persons, in particular the right of intimate, family and private life, in connection with the processing of personal data and the free circulation of these data.

The Authority has the following roles:

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.

- receives and examines the notifications on the processing of personal data;
- authorises the data processing in the situations mentioned by the law;
- receives and solves the complaints, intimations or requests of the natural persons and communicates the given solution;
- performs preliminary controls in case of special risks for the persons rights and freedoms;
- performs investigations at self-notification or at the reception of complaints or intimations;
- is consulted when normative acts regarding the protection of persons' rights and freedoms, concerning the personal data processing, are drafted;
- cooperates with the public authorities and public administration bodies, centralises and examines their annual reports regarding the people's protection concerning the processing of personal data;

The National Authority for the Supervision of Personal Data Processing prevents any violation of data protection files. In every hospital is named a DPO whose job is to work on protecting all private information and the files that are needed.

2.2.3.3 The enforcement of the GDPR in Romania

In order to implement the Regulation (EU) 2016/679 of the European Parliament on protection of natural persons regarding the processing of personal data and regarding the free movement of these data which repealed Directive 95/46/ EC (General Regulation regarding data protection), the laws mentioned above are also applied in the health sector.

National Health Insurance House (CNAS) has as its objective the defence of rights and fundamental freedoms of persons regarding the health domain. Because this is the institution that finances national medical health care, every hospital is bounded by contract to provide personal information of the patients. By law and contract it is mandatory for the hospitals to provide all this information for CNAS, information needed for expenses settlement. The purpose for collecting and using personal data is limited to ensure access to a package of basic medical services for the insured people allowing the efficient use of the National Health Insurance Fund (UNFASS). So, the institution has the obligation, established on the basis of Law 95/2006 on health reform to administer safely and only for the specified purpose, the personal data of insured persons.

For the processing of personal data, CNAS uses the Personal Numeric Code as an access key. CNAS processes the personal data of the insured persons in order to ensure the settlement of costs of medical services, medicines and medical devices.

We can mention the Electronic Health File (DES) that represents a public service provided by the National Health Insurance House (CNAS) for all patients who are insured in the social health insurance system. The Electronic Health File contains personalised clinical, biological, diagnostic and therapeutic data and information, that will be accumulated throughout the patient`s life, starting with the transmission of the first medical document to DES.

Law no. 45/2019 states that "the processing of personal data within DES (the Electronic Health File), as part of the Information Platform in health insurance, is carried out in compliance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Data Protection Regulation). Thus, the access of doctors to the medical data from the DES system will be only for emergency situations data summary; for more information, the patient approval will be necessary. Only doctors with an authorisation certificate can access an Electronic Health File (DES). The access of patients or their legal representatives to 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.

registered in the DES system will be achieved through a security matrix and an access password or on the basis of the national health insurance card with its associated PIN code and password.

In conclusion, such legislation as this is needed in any country and in any subject of business, even if it`s medical, insurance or construction, it is necessary for every citizen to know that their personal data and private information are protected.

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 Information Security for the Health Care Sector

The privacy and security of information is of prime importance to all individuals, government agencies and private sector organisations. Nowhere else is the protection of information a more sensitive issue than in the health care sector. Like many other industries, health care is becoming more efficient in delivering clinical results and more cost effective through the use of Information Technology (IT), including computers, applications, electronic networks and related technologies.

However, the use of these technologies and the increasing exchange of health information among health providers also pose a privacy and security risk to personal information (PI) and personal health information (PHI). Health information that is disclosed to unauthorised individuals, accessed incorrectly, tampered with, or lost could result in devastating impacts on patient health or even life.

There is no doubt that ICT will be a relevant player in the future of Healthcare, with predictive, preventive, personalised and participative medicine being the main pillars of future medicine. In this context, current technologies like telemedicine, home care systems, remote monitoring, wearable, big and smart data are just some examples of technologies that will be relevant to ensure the quality and sustainability of future health care models. In this environment, resilience of healthcare systems and the full patient ecosystem is a crucial need. Unlike other sectors, there is a direct and immediate impact on human life derived from the unavailability of certain healthcare systems. Therefore, resilience is a pillar in the generation of trust and confidence for patients in eHealth services. Conversely, in the last years we have seen an increase in attacks threatening and jeopardising this availability due to the increasing interconnection of healthcare systems, the stronger reliance on IT to execute basic healthcare activities and the growing interest of attackers in attacking health organisations because they have proven to be an easy target prone to paying requested ransoms in order to be able to regain control of their attacked systems.

Additionally, it is crucial to ensure the full confidence in the integrity of information being managed since false data can lead to invalid researches, incorrect diagnostics and ultimately even serious threats on the health of the patients. The need for confidence in the integrity of information is increasing mainly due to two current trends within the healthcare sector. On the one hand, the increasing amount of health information being gathered from patients, sometimes even in a continuous manner. On the other hand, the growing number of medical devices which are network connected and poorly protected. These devices introduce a triple threat to healthcare services. First, their lack of resilience due to the lack of adequate protections. Second, the serious threat to the health of the patients if information exchanged in and out of the medical device is intentionally or unintentionally altered. Third, due to their poor protection they introduce an entry point to the full health organisation's IT systems potentially compromising not only the availability of all systems as discussed before but also the integrity of information stored and exchanged.

Moreover, the obvious need within the healthcare environment is to provide confidence to patients that their information is being handled responsibly. A responsible management of private patients' information involves several aspects. Patients are full owners of their personal health information. They have the right to decide for which purposes such data is used, as well as who can use it and when. The privacy of this personal information is therefore crucial. Responsible management also ensures that the information is available when and where needed as long as this does not contradict the previous condition. Hence, secure health data exchange and access solutions have to be defined and available. On the other hand, data access and how to obtain relevant and valuable information from those data will be a key pillar for new advances like personalised medicine. Solutions that permit a simple, fast and accurate access to that information while at the same time preserving the first two clauses for responsible management would be a huge facilitator for the health research sector, empowering its growth.

Based on the above the main needs within the Health sector, regarding information security, can be summarised 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.

- Healthcare services' resiliency against cyber-attacks;
- Prevention against data leakage and loss of patient data and identity theft;
- Real-time security and dependability monitoring;
- Skills improvement – both technical and behavioural – of the personnel via innovative training techniques (The awareness level in cyber security aspects for all levels of healthcare personnel, e.g., nurses, technicians, administrative personnel and doctors, is an important aspect. The user is most often the weakest link when attacking the target);
- System availability and business continuity;
- Security mechanisms to achieve automatic recovery from a cyber-attack in the shortest time possible;
- Data security and integrity;
- Transparency of data usage;
- Harmonisation of services and problems with both roles in the hospitals and harmonising laws among different countries (especially in Europe);
- Include security and privacy by design in the evolution of hospital services;
- When new devices or systems are implemented, cyber security aspects should be taken into consideration beforehand;

Hospitals and healthcare organisations have evolved from a place of care to a delocalised network of care services. The development of Assisted Living systems is only one of the evolutionary aspects of the healthcare system. The long-term radical change of perspective goes under the name of "Patient Ecosystem". This evolution started a few years ago, but it is exponentially accelerating thanks to the evolutions of mobile services, the augmentation of the number of IoT devices, the wider use of information technology by patients and the increased impact of remote wellness solutions.

3.1 Information security Framework

The Information Security Framework ensures that the appropriate measures are implemented to protect the privacy and security of PI and PHI and to broadly educate the organisation about applicable laws and regulations governing information management, security and privacy. By implementing a security framework, healthcare providers improve their organisation management & support and facilitate the understanding of information security targets. In order to accomplish its goals, framework should establish an action plan, for implementing these security priorities that need to be adapted, according to the size and the complexity of each health care organisation. The minimum set of controls that must be implemented includes:

- Documentation of an analytic information security policy;
- Definition of information security roles and the corresponding responsibilities;
- Design of the information security framework review procedures;
- Selection and implementation guidelines of safeguards.

3.1.1 Information security policy

The information security policy is a document that defines the expected behaviours, responsibilities and rules that the organisation must follow and enforce for the safeguarding of information. The policy communicates management support for security activities and incorporates the mentality of information security practices within the organisation. Policy should focus on:

- Alignment of business strategy with the selected information security measures;
- Guidance and accountability for information security;
- Compliance with legislative, regulatory and any other requirements;
- Mitigation of risk 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.

- Exploiting efficiently all type of resources;
- Raise awareness on the importance of information security throughout the organisation.

3.1.1.1 Standards, Guidelines and Procedures

When the policy is drawn, supporting standards, guidelines and procedures must be selected/developed to serve the policy at a more detailed and specific level. The detail and depth of the standards and guidelines will depend upon the complexity and size of the healthcare organisation and its information systems. Of course this process must be constantly monitored to ensure completeness and relevance to the organisation.

3.1.1.2 Stakeholders in Policy Development

Information security policy development must take into account business objectives, technology restrictions, applicable legislation and regulations, security requirements and human behaviour. In order to integrate all aspects and be successfully implemented, policy should follow a consultation process with many reviews, revisions and stakeholder engagements.

3.1.2 Specifying Roles & Responsibilities

The information security framework must define the organisation's information security management structure, which will describe the assigning roles and their responsibilities for security throughout the organisation. The structure will ensure that information security activities are organised effectively and efficiently so that the users are aware of their security duties and acquire adequate training. Each organisation has its own unique requirements. Whereas large organisations follow the concept of segregation of duties, smaller organisations, mostly because of their limitations and needs, might assign multiple responsibilities to a single role. In this case, additional controls should be implemented to offset the risks.

3.1.3 Framework Review

All healthcare organisations should review (assess for gaps) their information security framework at planned intervals or when changes to the security program occur. The review allows the organisation identify opportunities for improvement and the need for changes to security (including the policy and other security control areas) in order to ensure the continuing suitability, adequacy and effectiveness of the information security framework.

3.1.4 Additional Safeguards

3.1.4.1 Confidentiality Agreements

A Confidentiality Agreement (CA) is a contract that requires one party, usually an employee or contractor, not to reveal confidential information that they acquire while working for the employer. CA communicates to employees their responsibility and accountability for protecting confidential information. All agreements should be signed, before any access is allowed to confidential information. CA must comply with all applicable laws and regulations and be easy to read and understand in order to help the signatory bodies to understand their ongoing obligations of confidentiality.

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.

3.1.4.2 Third Party Agreements

Most health care institutions require, to some degree, the assistance of third parties who may have access to information through physical channels (office, examination records in filing cabinets, laboratories, etc.), or through digital channels (Intranet, web applications, information systems etc.). A third party agreement is needed when an organisation is planning to disclose confidential or proprietary information to a third party. It is used to ensure that the third party is aware and accepts responsibility and accountability for protecting confidential information. It also demonstrates due diligence and may give the organisation legal recourse if the third party breaches the agreement.

3.2 Risk Management

Information Security Risk Management orchestrates all the necessary activities to ensure that security risks are identified, analysed, addressed and are consistent with business goals and objectives. These activities include the identification, assessment and appropriate management of current and emerging security risks that could cause disturbance, loss or harm to persons, business operations, information (including personal health data), systems or any other assets.

3.2.1 Objective

The objective of a risk assessment is to identify, prioritise and assess information security risks to which the healthcare organisation's assets are exposed so that the appropriate safeguards can be selected and implemented.

Risk assessments must be re-conducted when new elements are introduced within organisation, existing processes have changed, security breaches are identified, or even when there is an indication that the threat landscape is changing. Regardless the size of healthcare organisation, risk assessment can be used in order to ensure that changes in the business and technical environments are captured.

3.2.2 Risk Assessment

Initially, the objective of conducting risk assessments should be clearly presented. The scope must be defined (level: organisation, sector(s), department(s), project(s), resource(s) etc.) and provide all the dependencies, internally into the organisation, but also with all the external service providers.

Prior to starting the risk analysis organisation must specify the acceptable levels of risk tolerance. These thresholds provide guidance on how risks should be treated. Risks which fall below the threshold are acceptable to the organisation and may not require any actions. Risks which are assessed to be above the threshold will require actions which involve security controls intended to reduce the risk below the specific value.

Next step in conducting a risk assessment is the identification of assets and the valuation of them. A value must be assigned to each assets. As a list of assets in a complex health care organisation might prove to be much extended, introduction of (sub) categories can help make the risk assessment process easier. Any legal and/or other requirement related to each of the assets and to the organisation should be reflected in assets valuation. The outcome of this step is the list of assets and their values.

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.

Apart from asset analysis, risk assessment process should also evaluate whether any existing and/or planned safeguards are sufficient enough and if new ones need to be introduced in order to diminish the risk to acceptable levels.

Moving forward, threats and vulnerabilities should be identified and the likehood of occurrence should be assessed. All the possible threats that can emerge within organisation' environment must be identified in order to recognize the related vulnerabilities that may be exploited by these threats. For all these threats, the threat source and the threat target should be determined and the likelihood of occurrence should be assessed. Afterwards, the potential impact to the business if the vulnerability is exploited must be determined. Finally, the combination of threat likelihood and the estimation of impact provide the levels of risk.

3.2.3 Risk Treatment

Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories:[243]

- Reduction (optimize – mitigate)
- Sharing (transfer – outsource or insure)
- Avoidance (eliminate, withdraw from or not become involved)
- Retention (accept and budget)

Reduction: The risk is limited by implementing controls that minimize the adverse impact of a threat exploiting a vulnerability. More often than not, risk mitigation is the approach taken by most organisations.

Sharing: The risk or part of its impact is transferred to another party such as a supplier, through contracts, insurance and other mechanisms to limit the severity of consequences to the organisation or affected stakeholders.

Avoidance: The risk is avoided by changing the business scope, technical characteristics or usage of the information or system determined to be at risk.

Retention: The risk is accepted as is and operation of the system continues. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default.

Ideal use of these risk control strategies may not be possible. Some of them may involve trade-offs that are not acceptable to the organisation or person making the risk management decisions.

Once a decision has been made on how to treat the risks, a corrective action plan should be put into place outlining what must be done, by whom and by when. The action plan must be monitored for progress and completion.

Risk mitigation needs to be approved by the appropriate level of management. For instance, a risk concerning the image of the organisation should have top management decision behind it whereas IT management would have the authority to decide on computer virus risks. The risk management plan should propose applicable and effective security controls for managing the risks. A good risk management plan should contain a schedule for control implementation and responsible persons for those actions. Implementation follows all of the planned methods for mitigating the effect of the risks.

[243] Dorfman, Mark S. (2007). Introduction to Risk Management and Insurance (9 ed.). Englewood Cliffs, N.J: Prentice Hall. ISBN 0-13-224227-3.

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.

3.2.4 Risk Monitoring & Reviewing

In a constantly changing environment it is necessary to monitor risks, the effectiveness of the designed risk treatment plan and the evaluation of the implemented safeguards. Ongoing review is essential to ensure that the plan remains relevant and up to date.

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 Regulations and Platform-related Ethical Aspects

4.1 Compliance with the current national and EU legislation

Legislation concerning data protection and personal data processing must be taken into consideration, in order to ensure the compliance of the Sphinx platform with current European and national legal provisions.

4.1.1 Agreements, laws and regulations (including EU directive on data protection)

At a national level, Sphinx should be in alignment with the national legislation concerning personal data administration. Such pertinent legislation is presented for the pilot partners' countries in section 2. Moreover, EU and international legislation will be taken into account in order to avoid any data misuse. In case there are differences across applicable laws between two countries there must be a consensus regarding the final approach.

4.2 Acquiring agreements with third parties

Agreements should be acquired with third parties containing terms and conditions of cooperation.

4.3 Platform-related Ethical aspects

Privacy by design is a technical approach to a social problem.[244] Concerning limits of privacy by design, Danezis et al. (2014)[245] noted that there is a caveat: a significant part of the low-level privacy invasion is the direct result of the internal functioning of technical systems. Thus, while the incentives and will to invade privacy may be social problems, the actual ability to do so is a technical problem in many instances. Thus, dealing with it at the technology level is necessary.

4.3.1 Applying privacy design principles-ensuring appropriate level of sensitive personal data protection

Directive 2002/58/EC (ePrivacy Directive), still in effect until replaced by the ePrivacy Regulation, can be interpreted as a call for privacy by design while EU data protection law, Art. 29 Data Protection Working Party ask for and refer to privacy by design; there, practical aspects are also highlighted: "In practice, the implementation of the privacy by design principle will require the evaluation of several, concrete aspects or objectives. In particular, when making decisions about the design of a processing system, its acquisition and the running of such a system the following general aspects / objectives should be respected: Data

[244] Gürses, J. S. (2014). Can you engineer privacy? Communications of the ACM, 57(8):20–23

[245] Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, JH., Le Métayer, D., Tirtea, R., Schiffne, S. (2014). Privacy and Data Protection by Design–from policy to engineering. European Union Agency for Network and Information Security-ENISA Available at: https://www.enisa.europa.eu/publications/privacy-and-data-protection- by-design/at_download/fullReport

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.

Minimisation, Controllability, Transparency, User Friendly Systems, Data Confidentiality, Data Quality and Use Limitation".[246]

Before releasing the Sphinx platform it should be ensured that security policies are set appropriately and that the right measures to protect the data that users share with the platform. Some indicative tips for developers towards web security include, among others, review of data to collect and maintain and creation of secure users' credentials (usernames and passwords).[247]

4.3.2 Ensuring prevention of platform misuse (by any potential stakeholder of the platform)

The challenge for developers of an ICT platform is anticipating misuse and designing to prevent it. Providing that Sphinx might be dealing with sensitive data, it should be ensured that necessary standards and regulations are applied in order to prevent any misuse of application. Ways to prevent data misuse via the platform should be explored (such as monitoring of data access; monitoring of various stakeholders/users actions; and ensuring that the system is well-protected, as data misuse is considered a security breach and first and foremost it is a security concern[248]).

4.3.3 Transparent administration of log files (content; protection; access; destruction)

The first ethical dilemma mentioned in a popular article in InfoWorld[249] is about log files, what to save and how to handle them. It is noted that developers often keep records of everything, because this is the only way to debug a system. Log files, however, can expose information that users want kept secret. The mere existence of log files begs several ethical questions. Are they adequately protected? Who has access? When we say we destroy the files, are they truly destroyed? The crucial point, valid also for the Sphinx platform, is to decide what information is worth keeping, given the ethical risks of doing so.

4.3.4 Pre-define aspects of platform maintenance

Monitoring process and methodology for ensuring the smooth operation of the platform should be defined as well as the responsible organisation/authority to undertake the monitoring and consequently the reporting to data processor.

[246] Ibid.

[247] Source: https://www.owasp.org/index.php/Main_Page

[248] Source: https://www.ekransystem.com/en/blog/4-ways-detect-and-prevent-misuse-data

[249] Source: https://www.infoworld.com/article/2607452/application-development/12-ethical-dilemmas-gnawing- at-developers-today.html

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.

5 Ethical Provisions within Sphinx

5.1 Identify/recruit Research participants

First and foremost, the SPHINX project consortium commits to undertake its research in accordance with the Responsible Research and Innovation (RRI)[250] principles as well as in conformity with generally accepted ethical principles for scientific research, embodied e.g. in ALLEA (All European Academies)'s European Code of Conduct for Research Integrity[251].

Participants in research should have confidence in the experimenters. Good research is possible only if there is mutual respect and confidence between experimenters and participants. SPHINX will avoid situations where participants feel pressurised to take part in an experiment, for example, employees or clients. Direct payments are not to be considered for participation but other incentive mechanisms may be applied to encourage participation, as well as the adoption of certain behaviours. Such incentive mechanisms will not be designed to provoke excessive competition among participants.

In principle, the identification and recruitment of researchers will be based on the principle of information, and – to the highest possible extent – on the principle of prior, free, unambiguous and informed consent, insured by the Security Advisory Board. While the research is conducted, due consideration will be given to the ethical implications of their participation, such as dignity, health, non-discrimination, non-malevolence and well-being.

The trials of SPHINX will involve existing personnel of Polaris Medical Clinică de Tratament și Recuperare SA, Hospital do Espírito Santo de Évora and 5 Ygionomiki Periferia Thessalias & Stereas Elladas that are already working at the specific entities. For each trial, a specific business section and corresponding IT infrastructure will be selected. The selected trial areas in the entities will be defined according to the requirements and specifications.

Only healthy adult volunteers will be recruited in each pilot site. The recruitment method and informed consent procedures will be particularly stringent to ensure no coercion (not even soft or indirect) is exerted. The specific criteria for the selection of the volunteer participants are determined by the pilot requirements. There will be participants with various roles as described in the use cases of the project. More specifically, for the three End-user Pilots the research participants might hold the following positions: i) Chief Technology Officer; ii) Information Security Officer; iii) IT technician iv) SW Developers etc.

Also specific measures to protect the volunteer participants from a breach of privacy/confidentiality and potential discrimination will be applied, as it follows:

- ***Confidentiality***: The names of the employees participating in the trials will be never revealed in any document and their participation will not be communicated to their managers. As already stated above, all personal data stored during the industrial trials will completely and irreversibly anonymised and will be erased at the completion of the SPHINX Project. As an absolute minimum anonymised process, data will not contain any of the following, or codes for the following:
    - Name, address, phone/fax. number(s), e-mail address, full postcode
    - Any identifying reference numbers
    - Photograph or names of relatives
- ***Right to get more information about the trials:*** The volunteer employees can ask any questions about the trials at any time throughout the record. The Trial Responsible (one for each pilot trial foreseen in

[250] http://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation

[251] https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_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.

SPHINX) will be available to answer their questions, interests or concerns about the trial. During the trials, if any volunteer wish not to continue the trials he/she will have the right to do so, without having to give explanations and without being affected in any way.

- ***Informed Consent:*** A detailed informed consent will be created for each pilot trial, fully outlining the scope of the Trial and its purposes along with the data collected and analysed.

5.2 Ensuring data minimisation principle

Organisations must ensure that, in relation to all processing activities by default, they process only the minimum amount of personal data necessary to achieve their lawful processing purposes.

5.3 Informed Consent

The informed consent form, which each participant will be asked to complete prior to their participation in the pilots, aims at ensuring that the user accepts participation and is informed about all relevant aspects of the research project; it will be collected in written form after the users have been provided with clear and understandable information about their role (including rights and duties), the objectives of the research, the methodology used, the duration of the research, the possibility to withdraw at any time, confidentiality and safety issues, risks and benefits. Moreover, pertaining to non-academic participants, an information sheet has also to be drafted that it will clearly outline the nature of the current research project.

The basic elements of the Sphinx consent form will include information about the following:

- Data collected
- Usage of users' data by third parties
- Users' rights concerning their data
- Explanation of why Sphinx processes user data
- Contact details

5.4 Terms of Use

In order to ensure appropriate use of the Sphinx platform and at the same time to prevent misuse of the system or breach of confidentiality and data privacy, detailed "Terms of Use" is recommended to be drafted –although it is not mandatory by law- concerning all groups of main users taking into account their specific roles and level of access in the platform. Various templates are available online that may be used as a basis for preparing such a document for the needs of the specific platform (sample).

5.5 Code of Ethics of professionals that provide and administrate information

Main professional specialties to be involved in the Sphinx platform either as sources of data or as data administrators are already subjected in (national and international) professional codes of ethics. Such specialties may include but are not limited to universities and educational and training institutions, hospitals and healthcare organisations, public sector and public authorities, as well as private sector organisations and companies.

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.

5.6 Detailed instructions for data sharing

Detailed step-by-step instructions for data sharing, real-time messaging and collaborative tagging should be included in both, Terms of Use for organisations (educational and training institutions, public and private sector) as all of them are expected to be involved in these activities in the platform's collaborative space.

5.7 Safeguarding users' privacy and confidentiality of personal data

Sphinx should follow necessary procedures to ensure that all staff and others who have access to any personal information held by the Platform, are fully aware of and abide by their duties and responsibilities under the main EU legal framework.[252] Duties and responsibilities could be described either as part of the Terms of Use of main investigators' groups or in a separate "Data Protection and Confidentiality Policy" document which will be developed. Any data collection and storage involving humans will be strictly held confidential at any time of the research. This means in detail that:

- all the participants will be informed and given the opportunity to provide their consent to any monitoring and data acquisition process;
- no personal or sensitive data will be centrally stored. In addition, data will be scrambled where possible and abstracted in a way that will not affect the final project outcome;

5.7.1 Inform users about what personal information might be accessed, collected, how and why the information will be used and how they can control this use

This information should be clearly provided to users in the context of Privacy Policy; in addition, they should be informed on whether and how they can control the use of their personal data, providing them with appropriate tools.

5.8 Privacy policy

Sphinx is not expected to collect, store, and share personal data (e.g. names, email addresses, educational titles, skills, health records, interests etc.) of patients and healthcare professionals as well as of other groups of users within the healthcare domain, never the less, a privacy policy is mandatory, as the individual's rights are non-transferable and not subject to contractual waiver.

Therefore, an easily accessible privacy policy shall be drafted to inform users at least about

- what is Sphinx (identity and contact details)
- what personal data the platform collects and processes and why this is necessary (purpose)
- whether personal data will be disclosed to third parties (if yes, specifically to whom)
- what are their (users') rights, in terms of withdrawal of consent and deletion of data

Content of the privacy policy could be structured as follows:

[252] namely Data Protection Directive 95/46/EC; The ePrivacy directive 2002/58/EC as revised by 2009/136/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.

- Information Collected by the platform
- Information Shared with Third Parties
- Security
- Questions

Sphinx should follow necessary procedures to ensure that all staff and others who have access to any personal information held by the Platform, are fully aware of and abide by their duties and responsibilities under the main EU legal framework.[253] Duties and responsibilities could be described either as part of the Terms of Use of main stakeholders' groups or in a separate "Data Protection and Confidentiality Policy" document which will be developed.

[253] namely Data Protection Directive 95/46/EC; The ePrivacy directive 2002/58/EC as revised by 2009/136/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.

6 Summary and Conclusions

The purpose of this deliverable is to describe the legal and ethical framework pertaining to the gathering and processing of personal data and to identify restrictions in relation to privacy and data protection as well as access to personal information. As such, the European legislation was presented focusing mainly on the principles and rules set by the GDPR. The rules and regulations presented under the context of Chapter 2 led to the description and presentation of a general ethical framework (Chapters 3 & 4), pertaining to technical and non-technical aspects of the projected Sphinx platform and its individual components. This framework can be seen as the final set of legal and ethical guidelines regarding the information security that is generally and specifically applicable in healthcare sector.

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.