D8.1 SPHINX IPR Plan & IPR Management v1

WP8– Dissemination, Sustainability & Exploitation

Version: 1.00

SPHINX

A Universal Cyber Security Toolkit for Health-Care Industry

Disclaimer

Copyright message

Document information

Grant Agreement Number	826183	Acronym	SPHINX

Full Title	A Universal Cyber Security Toolkit for Health-Care Industry			
Topic	SU-TDS-02-2018 Toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures			
Funding scheme	RIA - Research and Innovation action			
Start Date	1st January 2019	**Duration**	36 months	
Project URL	http://sphinx-project.eu/			
EU Project Officer	Reza RAZAVI (CNECT/H/03)			
Project Coordinator	Dimitris Askounis, National Technical University of Athens - NTUA			
Deliverable	D8.1 SPHINX IPR Plan & IPR Management v1			
Work Package	WP8 – Dissemination, Sustainability & Exploitation			
Date of Delivery	**Contractual**	M9	**Actual**	M9
Nature	R - Report	**Dissemination Level**	P - Public	
Lead Beneficiary	VUB-LSTS			
Responsible Author	Dimitra Markopoulou	**Email**	Dimitra.Markopoulou@vub.be	
	Vagelis Papakonstantinou		Evangelos.Papakonstantinou@vub.be	
		Phone		
Reviewer(s):	Jason Mansell Rementeria (TECHNALIA), Carlos Goncalves (INCM)			
Keywords	Intellectual Property Rights, IPR Management			

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

Document History

Version	Issue Date	Stage	Changes	Contributor
0.10	18/07/2019	Draft	ToC	Dimitra Markopoulou / Vagelis Papakonstantinou (VUB-LSTS)
0.20	20/09/2019	Draft	Draft report for internal review	Dimitra Markopoulou / Vagelis Papakonstantinou (VUB-LSTS)
0.30	25/09/2019	Draft	Internal review audit, comments by TECHNALIA	Jason Mansell Rementeria (TECHNALIA)
0.40	25/09/2019	Draft	Internal review audit, comments by INCM	Carlos Goncalves (INCM)
0.50	28/09/2019	Draft	Incorporated review comments, content completion	Dimitra Markopoulou / Vagelis Papakonstantinou (VUB-LSTS)
0.51	29/9/2019	Draft	Quality Control	George Doukas (NTUA)
1.00	30/9/2019	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

Management of intellectual property rights plays an important role in all Horizon 2020 research projects. Based on guidance by the European Commission as well as the applicable EU law framework, aim of this report is to map the intellectual property options and tools available to the SPHINX project partners for protection of the IP created during the project execution. To this end the analysis includes a presentation of protection and exploitation methods of IP Rights (such as trademarks, patents, copyright and transfer and licensing agreements). This generic presentation is followed by a first approach of how SPHINX's results could be protected and exploited in the future. Given the early stage of project development, this report's main purpose is not to bring forward a final protection and exploitation plan but instead to provide project partners with timely and comprehensive guidance on efficient and competent protection of their project-related IP rights. This includes for instance advice on a dissemination policy, confidentiality and trade secret practices, as well as exploitation strategy.

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

Contents

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

Table of Tables

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

1 SPHINX IPR Management: The Grant Agreement and applicable EU provisions regarding Intellectual Property Rights

1.1 Introduction: IPR protection

Management of intellectual property rights plays an important role in all Horizon 2020 research projects. The European IP Helpdesk has issued a "guide to IP in Horizon 2020"[1] aiming to provide all participants with basic facts on central IP aspects that may arise in these projects. In the same context, the Commission has published a Recommendation[2] where it states that IP-related issues should be clarified at management level and as early as possible in the research project, ideally before it starts. IP-related issues include allocation of the ownership of intellectual property which is generated in the framework of the project (hereinafter "Foreground"), identification of the intellectual property which is possessed by the parties before starting the project (hereinafter "background") and which is necessary for project execution or exploitation purposes, access rights to foreground and background for these purposes, and the sharing of revenues.[3]

It is noted that IP rules of Horizon 2020 are built on the proven regulations of the previous FP7. However, there are some changes with an impact on the implementation and IP management of projects in Horizon 2020 with an emphasis on terminology. For instance, whereas results generated within the project were formally called "Foreground", in Horizon 2020 the term "Results" is now used.

In order to better understand what management of intellectual property includes, the first step would be to define "intellectual property" (IP). According to the Guidance for the implementation of the Code of practice incorporated in Commission's Recommendation "*Intellectual property is to be taken in the broadest sense, as encompassing any kind of new knowledge resulting from R&D activities (including inventions, software, databases, etc.), whether or not it is protected by formal IP rights such as patents*".

The glossary of the European IP Helpdesk defines intellectual property rights as any private legal rights that protect the creations of the human mind: inventions, literary and artistic works, and symbols, names, images, and designs used in commerce. They are commonly divided into two categories: Industrial Property Rights (e.g. patents, trademarks, industrial designs, geographical indications) and Copyright and Related rights (e.g. rights of the authors/creators and those of performing artists in their performances, producers of phonograms in their recordings, and those of broadcasters in their radio and television programs).

1.2 Rights and obligations related to Background

1.2.1 Definition of Background Knowledge

In Horizon 2020 all beneficiaries are obliged to define the pre-existing IP, know-how, knowledge or any additional data that is "needed for carrying out the project" (the so called "background").

[1] http://www.iprhelpdesk.eu/sites/default/files/2018-12/european-ipr-helpdesk-your-guide-to-ip-in-horizon-2020.pdf
[2] Commission Recommendation on the management of intellectual property in knowledge transfer activities and Code of Practice for universities and other public research organisations
[3] See https://ec.europa.eu/invest-in-research/pdf/download_en/ip_recommendation.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.

According to article 24.1 of the Grant Agreement (GA n.826183 — SPHINX), background means any data, know how or information -whatever its form or nature (tangible or intangible), including any rights such as intellectual property rights that:

a) is held by the beneficiaries before they acceded to the Agreement, and,

b) is needed to implement the action or exploit the results.

If one compares the new definition with the one included in the FP7 projects, the conclusion would be that no major changes have occurred. More specifically, in FP7 background is defined as "*the information and knowledge held by participants prior to their accession to the Grant Agreement, as well as any intellectual property rights which are needed for carrying out the project of for using the Foreground. Regarding intellectual property rights for which an application must be filed, only those intellectual property rights for which the application was filed before the accession of the participant to the Grant Agreement are included*".

In addition, it should be noted that the Background of a project partner is not limited to the information it owns, but also extends to any information or IPR which it holds – for instance through licensing agreements or material transfer agreements (MTAs).

1.2.2 Ownership of the Background and Access Rights

a. Ownership

Ownership of IP rights as per the EU glossary is defined as "*the state or quality of being an owner of a proprietary right. It enables its holder to exercise exclusive rights of use in relation to the subject matter of the IP and to restrict others from using these IP rights*".

The ownership of Background is not affected by participation in a Horizon 2020 research project. In other words, each project partner reserves all intellectual property rights on the background that it owns. The previous guide for FP7 projects[4] correctly draws attention to the issue of IPRs for which an application has to be filed (e.g. patents). The guide clarifies that the definition of background only includes those IPRs for which such an application was filed before acceding to the Grant Agreement (i.e. before starting the project). In other words, if an invention was made before starting the project, but a patent application for it was filed after starting the project, this application (and the resulting patent, if any) will not be considered as background. Therefore, if participants wish to avoid this, especially when, during their negotiations it appears that such an event is possible, they may agree to also include such later-filed IPRs in the definition of background.

b. Access rights

The definition provided by the EU glossary defines access rights for the purposes of Horizon 2020, as rights to use the project's results or background.

Article 25.2 of the Grant Agreement states that "Beneficiaries must give each other access -under fair and reasonable conditions- to background needed for exploiting their own results, unless the beneficiary that holds the background has -before acceding to the Agreement- informed the other beneficiaries that access to its background is subject to legal restrictions or limits, including those imposed by the rights of third parties (including personnel)".

[4] https://ec.europa.eu/research/participants/data/ref/fp7/89593/ipr_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.

Article 25.3 of the Agreement regulates the access rights for other beneficiaries for exploiting their own results and reads as follows: "The beneficiaries must give each other access -under fair and reasonable conditions- to background needed for exploiting their own results, unless the beneficiary that holds the background has -before acceding to the Agreement- informed the other beneficiaries that access to its background is subject to legal restrictions or limits, including those imposed by the rights of third parties (including personnel)".

According to article 25.3 of the Agreement '**Fair and reasonable conditions**' means appropriate conditions, including possible financial terms or royalty-free conditions, taking into account the specific circumstances of the request for access, for example the actual or potential value of the results or background to which access is requested and/or the scope, duration or other characteristics of the exploitation envisaged. Participants may of course opt for a combination of the two (for example royalty-free for further research purposes and, as is often the case, on fair and reasonable conditions for other use purposes).

Unless agreed otherwise, access rights do not include the right to sub-license. Access rights may be requested until the end of the project whereas requests for access may be made -unless agreed otherwise- up to one year after the period set out in Article 3 of the Grant Agreement, that is 36 months as of 1st January 2019.

The partners in the SPHINX consortium have included in the Consortium Agreement (in its Attachment 1) the Background for the Project, as well as the specific access rights that apply to such Background (including possible legal restrictions or limits). Any project partner may add further Background to Attachment 1 during the Project by written notice to the other Parties. The CA clarifies in its article 9.2.3 that access rights are granted on a non-exclusive basis.

1.3 Rights and obligations related to Results

1.3.1 Definition

As already mentioned above, in the Horizon 2020 projects the term "Foreground" has been replaced by the term "Results".

Results are defined as: "*Any tangible or intangible output of the action, such as data, knowledge and information whatever their form or nature, whether or not they can be protected, which are generated in the action as well as any attached rights, including intellectual property rights*[5]."

The previous definition defined foreground rights as "the results, including information, materials and knowledge, generated in the project, whether or not they can be protected. It includes intellectual property rights (IPRs such as rights resulting from copyright protection, related rights, design rights, patent rights, plant variety rights, rights of creators of topographies of semiconductor products), similar forms of protections (e.g. sui generis right for databases) and unprotected know-how (e.g. confidential material). Thus, Foreground includes the tangible (e.g. prototypes, micro-organisms, source code and processed earth observation images) and intangible (IP) results of a project. Results generated outside a project (i.e. before, after or in parallel with a project) do not constitute Foreground".

In the European IP Helpdesk guide the following wording is used to define results: "In a nutshell, results encompass all project outcomes that may be used by the project partners or other relevant stakeholders outside the project. They have the potential to be either commercially exploited (e.g. concrete products

[5] See Grant Agreement, article 26.1

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.

or services) or lay the foundation for further research, work or innovations (e.g. novel knowledge, insights, technologies, methods, data)".[6]

1.3.2 Ownership of the Results and Access Rights

a. Ownership

According to Article 26.1 of the Grant Agreement, results are owned by the beneficiary that generates them. As far as joint ownership is concerned, Article 26.2 states that two or more beneficiaries own results jointly if a) they have jointly generated them and b) it is not possible to i) establish the respective contribution of each beneficiary, or (ii) separate them for the purpose of applying for, obtaining or maintaining their protection (see Article 27).

In order to be able to prove ownership (as well as the date of generation) of Foreground, it is strongly recommended that all project partners maintain documents showing the development of the generation of knowledge or results, in accordance with proper standards.

In order to minimise the possibility of third parties and in particular employees and other personnel raising any claim on IP rights to Foreground, it is recommended that participants reach an agreement with them in advance. Such agreements may for instance involve a formal transfer of ownership, or at least the granting of appropriate access rights (with a right to sublicense).

For academic institutions, this is especially relevant regarding (a) "non-employees" such as students (both undergraduate and postgraduate, e.g. PhD students), and (b) researchers in those countries having a specific type of "professor's privilege" regime (according to which the researchers concerned may have some personal rights to the results of university research).

b. Access rights

Access rights to results are regulated under articles 31 and 25 of the Grant Agreement. As per article 31, article 25 that regulates access rights to background applies also to Foreground 25 also apply to results. Therefore, access rights mean rights to use results under the terms and conditions of the Grant Agreement.

It is noted that access to another participant's Foreground and Results is only to be granted if the requesting participant needs that access in order to carry out the project or use its own results. Assessing whether or not access rights are needed must take place on a case by case basis and always in good faith.

The Consortium Agreement includes specific terms regarding the partners' access rights to software (see art. 9.8 of the CA)

The table that follows, as this has been included in the IPR Helpdesk of the EU, summarises the conditions concerning the granting of access rights under the Grant Agreement[7]

Purpose	Access to background	Access to results
Implementation of the project	Royalty-free, unless otherwise agreed by participants before their accession to the grant agreement	Royalty-free

[6] http://www.iprhelpdesk.eu/sites/default/files/2019-05/Brochure_Making_the_Most_of_Your_H2020_Project_web.pdf
[7] http://www.iprhelpdesk.eu/sites/default/files/2018-12/european-ipr-helpdesk-your-guide-to-ip-in-horizon-2020.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.

Purpose	Access to background	Access to results
Exploitation of project results	Subject to agreement, access rights shall be granted under fair and reasonable conditions (which can be royalty-free)	

Table 1: Access Rights under Grant Agreement

1.4 Protection of exploitation of Results

1.4.1 Protection of Results

As per article 27.1 of the Grant Agreement each beneficiary must adequately protect its results if two conditions apply:

a. the results can reasonably be expected to be commercially or industrially exploited, and

b. protecting them is possible, reasonable and justified.

1.4.2 Exploitation of Results

The EU IP Glossary defines Exploitation as **"**The utilisation of results in further research activities other than those covered by the action concerned, or in developing, creating and marketing a product or process, or in creating and providing a service, or in standardisation activities."

Article 28.1 of the GA sets the beneficiaries' obligation to take measures aiming to ensure exploitation of their results by:

(a) using them in further research activities (outside the action);

(b) developing, creating or marketing a product or process;

(c) creating and providing a service, or

(d) using them in standardisation activities.

1.5 Dissemination

According to the EU IP glossary dissemination is defined as "The public disclosure of the results by any appropriate means (other than resulting from protecting or exploiting the results), including by scientific publications in any medium."

As per article 29(1) of the GA each beneficiary must — as soon as possible — 'disseminate' its results by disclosing them to the public by appropriate means (other than those resulting from protecting or exploiting the results), including in scientific publications (in any medium). This does not change the obligation to protect results in Article 27, the confidentiality obligations in Article 36, the security obligations in Article 37 or the obligations to protect personal data in Article 39, all of which still apply.

It should be taken into consideration that a beneficiary that intends to disseminate its results must give advance notice to the other beneficiaries of — unless agreed otherwise — at least 45 days, together with sufficient information on the results it will disseminate. Any other beneficiary may object within — unless agreed otherwise — 30 days of receiving notification, if it can show that its legitimate interests in relation to the results or background would be significantly harmed. In such cases, the dissemination may not

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

take place unless appropriate steps are taken to safeguard these legitimate interests. If a beneficiary intends not to protect its results, it may — under certain conditions (see Article 26.4.1) — need to formally notify the Commission before dissemination takes place.

1.6 Transfer and licensing of Results

1.6.1 Transfer

Each partner may exploit its results by means of either (a) a transfer or (b) a license.

Transfer is regulated under article 30.1 of the GA which reads as follows: "Each beneficiary may transfer ownership of its results. It must however ensure that its obligations under Articles 26.2, 26.4, 27, 28, 29, 30 and 31 also apply to the new owner and that this owner has the obligation to pass them on in any subsequent transfer. This does not change the security obligations in Article 37, which still apply. Unless agreed otherwise (in writing) for specifically-identified third parties or unless impossible under applicable EU and national laws on mergers and acquisitions, a beneficiary that intends to transfer ownership of results must give at least 45 days advance notice (or less if agreed in writing) to the other beneficiaries that still have (or still may request) access rights to the results. This notification must include sufficient information on the new owner to enable any beneficiary concerned to assess the effects on its access rights. Unless agreed otherwise (in writing) for specifically-identified third parties, any other beneficiary may object within 30 days of receiving notification (or less if agreed in writing), if it can show that the transfer would adversely affect its access rights. In this case, the transfer may not take place until agreement has been reached between the beneficiaries concerned".

The CA further clarifies in its term 8.3. (transfer of results) that each Party may transfer ownership of its own Results following the procedures of the Grant Agreement Article 30. It also states that it may identify specific third parties it intends to transfer the ownership of its Results to in Attachment (3) to this Consortium Agreement. The other Parties hereby waive their right to prior notice and their right to object to a transfer to listed third parties according to the Grant Agreement Article 30.1. At the same time the transferring Party shall, at the time of the transfer, inform the other Parties of such transfer and shall ensure that the rights of the other Parties will not be affected by such transfer. Any addition to Attachment (3) after signature of this Agreement requires a decision of the Management Board.

1.6.2 Licensing

Licensing is regulated under article 30.2: "Each beneficiary may grant licences to its results (or otherwise give the right to exploit them), if: (a) this does not impede the access rights under Article 31 (see above under 3.1.2) and (b) not applicable. In addition to Points (a) and (b), exclusive licences for results may be granted only if all the other beneficiaries concerned have waived their access rights (see Article 31.1). This does not change the dissemination obligations in Article 29 or security obligations in Article 37, which still apply".

1.7 Confidentiality

Article 36.1 of the GA sets the beneficiaries' obligation to maintain confidentiality during implementation of the action and for four (4) years after the end of the Project. In particular, the parties must keep confidential any data, documents or other material (in any form) that is identified as confidential at the time it is disclosed ('confidential information'). If information has been identified as confidential only

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.

orally, it will be considered to be confidential only if this is confirmed in writing within 15 days of the oral disclosure. Unless otherwise agreed between the parties, they may use confidential information only to implement the Agreement. The beneficiaries may disclose confidential information to their personnel or third parties involved in the action only if they: (a) need to know to implement the Agreement and (b) are bound by an obligation of confidentiality.

Furthermore, the same article mentions the conditions under which the confidentiality obligations no longer apply, namely if:

(a) the disclosing party agrees to release the other party;

(b) the information was already known by the recipient or is given to him without obligation of confidentiality by a third party that was not bound by any obligation of confidentiality;

(c) the recipient proves that the information was developed without the use of confidential information;

(d) the information becomes generally and publicly available, without breaching any confidentiality obligation, or,

(e) the disclosure of the information is required by EU or national law.

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 Protection and exploitation of the SPHINX Results: A first evaluation

2.1 Project's description and objectives

SPHINX is described as a toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures. More particularly, SPHINX aims to introduce a Universal Cyber Security Toolkit, thus enhancing the cyber protection of Health IT Ecosystem and ensuring the patient data privacy and integrity. SPHINX toolkit will provide an automated zero-touch device and service verification toolkit that will be easily adapted or embedded on existing, medical, clinical or health available infrastructures, whereas a user/admin will be able to choose from a number of available security services through SPHINX cyber security toolkit. The SPHINX toolkit will enable service providers to specify complete services and sell or advertise these through a secure and easy to use interface. SPHINX software will form a Cybersecurity Incident Collection Platform that performs network analysis and deep packet inspection for suspicious pattern recognition;

SPHINX Objectives could be summarised to the following:

1. To provide a novel information security awareness ecosystem capable to detect and quickly and effectively respond to sophisticated cyber-attacks.
2. To implement a shared sandbox environment for medical equipment testing. SPHINX Sandbox will be a security mechanism for separating running programs, usually in an effort to mitigate medical device failures or software vulnerabilities from spreading.
3. To implement and provide Opensource, an automated toolkit for assessing devices and services for the health and care domain.
4. To offer a novel architecture for the provision of highly adaptive cyber security services and intelligence dynamically adjusted to the changing needs of each user.
5. To develop innovative methods and technologies for data analytics and open APIs to support connectivity and intelligence.
6. To apply behavioural analysis to detect and assess the risk level from organisational processes and/or individual behaviours with the aim to automatically implement appropriate incentives for behavioural change and awareness enhancement.
7. To offer a novel platform for the provisioning of highly adaptive cyber security services and intelligence, dynamically adjusted to the changing needs of involved end users.
8. To design an integrated and advanced holistic security/privacy toolkit in order to cover the demanding user needs.
9. To validate the proposed technology and business framework through pan-European demonstrations in two different scenarios.
10. To perform all required activities, e.g. formulate the appropriate business models and settle IPR procedures for pushing the outcome of this action as a commercial product in the relevant SME market.

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 Protection of SPHINX's Results

2.2.1 IP protection toolset

Project partners should, during the SPHINX project, examine and evaluate the means of protection that may apply to their results. IP protection toolset in the European Union for any IP subject matter includes:

a. Copyrights;

b. Patents;

c. Industrial designs;

d. Trade secrets;

e. Trademarks.

A. Copyright

Copyright protects works such as: literary works, novels, song lyrics, newspaper articles, computer programs, some types of databases, musical works, artistic works, paintings, photographs, sculptures, architectural designs, technical drawings, diagrams, maps, logos.

Copyright acquisition and protection is automatic in the EU, as well as in every country that is a signatory to the Berne Convention[8]. Copyright, therefore, arises from the moment of the work's creation. Therefore, no registration or other formality is required. Nevertheless, if a copyright owner feels the need to inform any third parties the existence of copyright ownership, then the copyright owner may mark copyrighted works with a copyright notice, such as the copyright symbol (©), followed by the owner's name and year of the work's protection.

In order for a work to qualify for copyright protection, a work must:

- be original, in the sense that it is the author's own intellectual creation;
- exist in some physical form (this requirement is only applicable in some Member States as it is subject to national laws).

With regard to **computer programs** in particular, Directive 2009/24 seeks to harmonise Member States' legislation in the field of legal protection of computer programs. Member States protect computer software as such by copyright, by analogy to the protection given to literary works within the meaning of the Berne Convention for the Protection of Literary and Artistic Works.

It is pointed out that the functionality of a computer program or the format of data files used in a computer program or the programming language are not protected. What is protected by copyright is the source code and its interface.

Patentability of computer programs is examined below under b.

b. Patents

A patent is a legal title granting its holder the right – in a particular country and for a certain period of time – to prevent third parties from exploiting an invention for commercial purposes without

[8] https://www.wipo.int/treaties/en/ip/berne/

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.

authorisation. Unlike copyright, an invention needs to be registered in order to be protected with a patent.

In Europe, the European Patent Convention (EPC) has established a single European procedure for the grant of patents on the basis of a single application. European patents are granted for inventions that are:

- new;
- involve an inventive step, and
- are susceptible of industrial application.

An invention is considered to be new if it does not form part of the state of the art. An invention is held to involve an inventive step if it is not obvious to the skilled person in the light of the state of the art. An invention can belong to any field of technology. The EPC does not define the meaning of invention; however, it provides a non-exhaustive list of subject-matter and activities that may not be regarded as inventions. Prominent among them, and the one that applies to the SPHINX Project, is computer programs.

Article 52 of the European Patent Convention excludes software from patentability to the extent that a patent application relates to a computer program "as such". A distinction is, however, made between "software patents" which are excluded according to Article 52 EPC and so- called computer-implemented inventions which are accepted at the European Patent Office. In this respect, "computer-implemented inventions" can be defined as inventions whose implementation involves the use of a computer, a computer network or other programmable apparatus, having one or more features realised by means of a computer program. It seems therefore that patentability must not be denied merely because a computer program is involved. A project partner could seek patent protection if the subject matter of its invention as a whole, i.e. a machine with related software, has a technical character - this technical character must be present in all variants covered by the patent claim.

c. Industrial designs

A design is the outward appearance of a product or part thereof resulting, in particular, from the characteristics of the lines, contours, colours, shape, surface, structure and/or materials of the product itself and/or its ornamentation.

A design is protected by an exclusive right if it is new and has individual character. A design is considered new if, on the date on which the application for registration has been filed, no identical design has been made available to the public. A design is considered to have an individual character if the overall impression that it produces on an informed user differs from the overall impression made by any design available to the public before the date of filing of the application for registration.

In the EU, one may obtain a Community design registration valid in all member countries through a single application, which can be filed directly in the European Union Intellectual Property Office (EUIPO).

d. Trade secrets

Patents and trade secrets represent two of the most common methods in the technology sector to protect intellectual property. However, the degree of protection provided by trade secrets is lower than the one provided by patents. This is because, in the case of trade secrets, the protection is dependent on the confidential status of a trade secret. Once a trade secret is disclosed or revealed, it loses its secret status and therefore the protection. Furthermore, trade secrets do not confer "proprietary rights",

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

meaning that the holder of a trade secret does not have exclusive rights over the information. On the other hand, unlike patents trade secrets do not need to be novel nor need registration.

A trade secret is confidential information and know-how in the context of business, commerce or trade that is not protectable or cannot be protected properly through patents. In order for a given piece of information to classify as a trade secret, it has to meet all of the following requirements:

1. it is secret, in the sense that it is not known or readily accessible to a wide circle of persons;
2. it has commercial value because it is secret; and
3. it has been subject to reasonable steps under the circumstances, by the person in control of the information, to keep it secret.

Trade secrets may include, indicatively:

- early-stage inventions
- manufacturing processes
- lists of suppliers and clients
- business methods
- business planning
- computer programs
- market analyses manufacturing methods
- product technology
- computer databases
- formulae and recipes ingredients

Until 2016 there were no harmonised laws related to the protection of trade secrets at the European Union (EU) level. However, on June 2016 Directive (EU) 2016/943 of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure was adopted.

e. Trademarks

Trademarks are signs used in trade to identify products and services. More specifically, a trademark may consist of any sign, particularly words, including personal names, designs, letters, numerals, the shape of goods or of their packaging, or sounds, provided that they can be clearly represented on the register and are capable of distinguishing the goods or services of your undertaking from those of other undertakings.

Trademarks can be protected through registration at national, EU or international level.

European Union Trademarks (EUTMs) in particular are issued by the European Union Intellectual Property Office (EUIPO). Once registered with the office EUTM grants its owner exclusive rights in all current and future Member States of the European Union through a single registration, filed online. It is valid for 10 years and can be renewed indefinitely, 10 years at a time for each renewal.

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 Applicability of the IP protection toolset onto SPHINX Results

Each beneficiary under a H2020 project has an obligation to examine the possibility of protecting its results and protect them adequately **if such results can reasonably be expected to be commercially or industrially exploited.** Nonetheless, the reference to industrial or commercial applicability means that not all results have to be protected. For instance, for results that are not expected to be commercially or industrially exploited or whose protection is impossible under European Union or national law or not justified, there is no such obligation.

Furthermore, when deciding whether to protect results or not, the beneficiaries must also consider the other beneficiaries' legitimate interests and conform to all the relevant legal provisions, including the provisions set out in the Consortium Agreement. Where a participant does not intend to protect a result, it is also best practice to consider offering to transfer it to other consortium partners or third parties established in a Member State or associated country, better positioned for the exploitation of the results and willing to seek their protection.

Finally, if valuable results are left unprotected, the Commission may take over their ownership.

In the case of the SPHINX results, their commercial or industrial exploitation is expected. Therefore, protection of such results should be evaluated by the SPHINX Partners at this early stage of the project. **It is pointed out that this report aims to provide some basic guidelines to the Project's Partners in order to better understand the Intellectual Property they already have or they will develop during the Project's life and accordingly to examine the means to protect it. An IPR management plan in its final form will be examined under deliverable D8.11 that is due in M36, when the project has reached its final stage.**

In this context SHPINX results could be protected as follows:

a. Partners' Foreground

At partner level, each partner should apply an IP policy within its company in order to evaluate and protect its foreground.

SPHINX includes the design of modules (software) and consequently copyright protection applies in all cases where a partner develops software.

Patent protection is an option when inventions are involved however the patentability of the Partner's Foreground in the case of SPHINX, given that it consists, to a great extent, of software needs to be evaluated by each partner in the context of its business. One way of demonstrating patentability is to identify the state of the art by conducting not only a bibliographic search in classical scientific literature but also a search in patent databases.

Dissemination of project results is directly connected to their protection. Participants in Horizon 2020 projects commit to disseminate projects results as soon as possible by appropriate means. It is very important however that each partner considers the possibility of protecting any results that are capable of commercial or industrial exploitation before any dissemination activity. At the same time, it is essential that all partners consult with each other – especially in case of joint ownership of results – before any public disclosure. Evidently, no dissemination at all may take place if it is intended to protect the Foreground as a trade secret. **Designing and applying a dissemination and exploitation plan at the**

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

beginning of the Project and keeping this plan updated and reviewed throughout the project's duration will help partners to exploit the results to their fullest potential.

It is pointed out that the European Commission promotes the overall concept of **Open Research by supporting open access** in its framework programmes. Open access however will not affect the intellectual property generated by the Partner's research results. The decision on whether to seek protection for intellectual property rights is made before deciding whether or not to publish open access. Therefore, research results can only be published after an application for IP protection (e.g. patent application) has been filed. Similarly, the author will retain the publication's copyright, even if it is open access. The protection of research results and their commercial exploitation (for example through patenting) is still guaranteed.

In this context and given the early stage of the SPHINX Project, it is recommended that all partners treat their know-how and information as trade secrets. Some steps that are suggested to this end include:

- assessing the company's valuable confidential information;
- developing an internal trade secret policy;
- document marking;
- employee activity monitoring;
- employee training;
- storing confidential information safely;
- creating employee awareness of the importance of keeping trade secrets safe;
- concluding non-disclosure agreements in the case where trade secrets must be discussed with business partners;
- including non-disclosure clauses within agreements such as licence agreements, consortium agreements or partnership agreements, where the exchange of confidential information is very likely and/or necessary;
- identify trade secrets in the company;
- keep records of the trade secrets;
- define company policy regarding trade secrets;
- enter into NDAs/non-solicitation agreements with employees, contractors, external partners, and visitors;
- use technical measures such as passwords, locks, badges and other policies to physically protect your trade secrets;
- design a dissemination plan;
- organise background and results;
- examine dissemination channels, for instance: Scientific and non-scientific publications, Conferences, Networking events and business fairs, Project websites, Communication material (such as posters, leaflets), Social Media, Open Access.

By applying these measures, any Foreground developed in the context of the SPHINX project will be adequately protected until the Partners decide what further measures of protection they need to undertake and what is the best way to disseminate these results to the public.

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. SPHINX Results

Both the project's description and objectives, as provided above under 2.1, give the basic guidelines regarding the results that are anticipated to be produced during SPHINX. In this context, the results will mainly include a security solution/application that will operate on a platform, the SPHINX Services platform, and will be provided to end users as a service (the SPHINX toolkit). At the same time, the individual components of the proposed solution will find their way to the market as a stand-alone solution or bundled with others.

Protection of SPHINX Technology will be examined in more detail at a later stage of the SPHINX Project. Given the early stage of Project execution, any suggestions with regard to the method of protection of SPHINX results, for instance whether the SPHINX Technology could be patentable, could prove irrelevant. Such analysis will become possible only after the end-product has been formulated, at least as far as its basic characteristics are concerned.

It is for this reason that it is strongly recommended that all Partners adopt the necessary measures to protect their Results, in order to keep all their IP protection options and tools open for future evaluation at a time when definitive recommendations will be possible.

2.3 Exploitation

Proper exploitation of the results of a project is essential and will allow the project's beneficiaries to profit from marketing and commercialisation of the intellectual assets created during the project. On this basis an exploitation strategy must be in place even from the beginning of the project. However, given the fact that in many cases the majority of the expected results are available towards the end of the project and exploitation obligations remain in effect up to four (4) years after the project end, finalisation and implementation of exploitation measures are expected at the concluding phase of the project.

As with protection measures, this report aims to present preliminary guidance on exploitation methods that the partners should take into consideration while developing the SPHINX solution. An exploitation plan in a final version is expected to be presented in version 2 of SPHINX IPR Plan and IPR Management (Deliverable D8.11).

The Grant Agreement includes a preliminary list of potential exploitable results/ assets of SPHINX. The list will be reviewed and updated during the project implementation.

Project Result/asset	Type of Result	Owner	IPR Strategy and Foreseen Exploitation
SPHINX Common Integration Platform	Product	ICOM	Licensed for stand- alone solution/Collaboration with Cyber Security Toolkit
SPHINX DSS Module & Analytic Engine	Product & service	KT	Licensed for stand- alone solution. Free use by all SPHINX partners
Anomaly Detection	Service	SIVECO	Licenced for stand- alone solution or for integration into cybersecurity applications

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.

Project Result/asset	Type of Result	Owner	IPR Strategy and Foreseen Exploitation
Information Fusion and Multilevel Visualisation	Service	KT/ViLABS	Licenced for stand- alone solution or for integration into cybersecurity applications
Forensic Data Collection Engine	Product & service	NTUA	Licenced for stand- alone solution or for integration into cybersecurity applications
Vulnerability Assessment as a Service & Automated Cybersecurity Certification	Product & service	TEIC/INCM	Licenced for stand- alone solution or for integration into cybersecurity applications
Common Cyber Security Toolkit	Product & service	TEIC/FINT	Licenced for stand- alone solution or for integration into cybersecurity applications
Real time cyber risk assessment models	Product & service	NTUA	Licenced for stand- alone solution or for integration into cybersecurity applications
Blockchain Based Threats Registry	Product & service	TECNALIA	Licenced for stand- alone solution or for integration into cybersecurity applications
AI - Honeypot	Product & service	FINT	Licenced for stand- alone solution or for integration into cybersecurity applications
SPHINX Sandbox	Product & service	PDMFC	Licenced for stand- alone solution or for integration into cybersecurity applications
SPHINX Enabling APIs	Product & service	EDGE	Licenced for stand- alone solution or for integration into cybersecurity applications
ML empowered intrusion detection using Honeypots' data	Product & service	AIDEAS	Licenced for stand- alone solution or for integration into cybersecurity applications
Encryption Techniques- Homomorphic Techniques	Product & service	TEC	Licenced for stand- alone solution or for integration into cybersecurity applications
SPHINX SIEM	Product & service	PDMFC	Licenced for stand- alone solution or for integration into cybersecurity applications

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

Table 2: List of potential exploitable results

In this context, exploitation may include measures (indicatively):

- to use research results in further research activities of an organisation either internally and/or as background to be brought into a new collaborative research project;
- to create new or contribute to on-going standardisation activities;
- to develop and create new services and/or products;
- to Commercially exploit the research results by means of licensing, assignment, joint venture, spin-off or franchising.

Some of the questions that may be raised at this stage of the Project in order to help the partners to better evaluate possible means of the Project's exploitation, as these are included in the Commission's IP Helpdesk-Making the most of your 2020 Project, include the following:

- What are the (expected) key exploitable results of the project?
- How is the value for further use going to be assessed?
- Which IP protection and IP management measures have been laid down for expected results?
- How will project partners address the issue of (joint) ownership of results and the management of exploitation activities – especially for jointly owned results?
- How are the results going to be used to a) address the call topic challenges and expected impacts, and b) for further uses?
- Who are the main innovators within the consortium to drive commercial exploitation?
- Which (other) results will be produced and could be exploited by people or organisations outside the project – under which terms and conditions?
- What are potential additional application areas (even outside the project's field of research) that could benefit from its developments?
- What impact do your results have for everyday life? How could society benefit from your work?
- What would be the consequences for future policymaking?
- What are the market & customers' needs and wants?
- What are the key messages related to your results that you wish to communicate? (e.g. What is new? Why is it important?)
- What are your objectives and who are your target audiences you want to reach with your communication activities, and consequently, what are the appropriate communication tools?

It is recommended that all partners who participate in the SPHINX Project address the above questions within their respective organisations. Timely elaboration of the above as regards project execution, as well as having in place a first draft of an IPR protection plan will contribute decisively to optimised exploitation of project Results.

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 Conclusion

This report aims at highlighting the main intellectual property rights issues that may arise during the SPHINX project lifetime. The analysis includes a presentation of protection and exploitation methods of IP Rights (such as trademarks, patents, copyright and transfer and licensing agreements respectively). A general presentation is followed by a first approach of how SPHINX's results could be protected and exploited in the future. Given the early stage in project execution this report's main purpose is not yet to come up with a detailed protection and exploitation plan but instead to provide to project partners guidance regarding how they could efficiently manage their project-related IP. This includes advice on a dissemination policy that the partners could apply, confidentiality and trade secret practices, as well as preliminary guidance on Results' exploitation planning. A more concrete IPR management plan is scheduled for month 36 of the Project and shall be presented under Deliverable D8.11.

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

Annex I: **References**

European Commission, Commission Recommendation on the Management of Intellectual Property in Knowledge-Transfer Activities and Code of Practice for Universities and other Public Research Institutions

https://ec.europa.eu/invest-in-research/pdf/download_en/ip_recommendation.pdf

European Commission, Guide to Intellectual Property Rules for FP7 Projects

https://ec.europa.eu/research/participants/data/ref/fp7/89593/ipr_en.pdf

European IP Helpdesk, Your Guide to IP in Horizon 2020

http://www.iprhelpdesk.eu/sites/default/files/2018-12/european-ipr-helpdesk-your-guide-to-ip-in-horizon-2020.pdf

European IP Helpdesk, Making the most out of your H2020 project

http://www.iprhelpdesk.eu/sites/default/files/2019-05/Brochure_Making_the_Most_of_Your_H2020_Project_web.pdf

European IPR Helpdesk, Fact Sheet – Trade Secrets: An efficient tool for competitiveness

https://www.iprhelpdesk.eu/sites/default/files/newsdocuments/Fact-Sheet-Trade-Secrets.pdf

European Patent Office, How to Get a European Patent – Guide for Applicants

https://www.epo.org/applying/european/Guide-for-applicants.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.