SECUREHOSPITALS.EU

RAISING AWARENESS ON CYBERSECURITY IN HOSPITALS ACROSS EUROPE AND BOOSTING TRAINING INITIATIVES DRIVEN BY AN ONLINE INFORMATION HUB

POPD – Requirement No. 2

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 826497.

PROJECT DESCRIPTION

Acronym: **SecureHospitals.eu**

Title: **Raising Awareness on Cybersecurity in Hospitals across Europe and Boosting Training Initiatives Driven by an Online Information Hub**

Coordinator: INTERSPREAD GmbH
Reference: 826497
Type: CSA
Program: HORIZON 2020
Theme: eHealth, Cybersecurity
Start: 01. December, 2018
Duration: 26 months
Website: https://project.securehospitals.eu/
E-Mail: office@securehospitals.eu

Consortium: **INTERSPREAD GmbH**, Austria (INSP), Coordinator
Erasmus Universiteit Rotterdam, Netherlands (EUR)
TIMELEX, Belgium (TLX)
Fundacion Privada Hospital Asil de Granollers, Spain (FPHAG)
Cooperativa Sociale COOSS Marche Onlus, Italy (COOSS)
Arbeiter-Samariter-Bund, Austria (SAM)
Johanniter International, Belgium (JOIN)
European Ageing Network, Luxembourg (EAN)

DELIVERABLE DESCRIPTION

Number:	**D7.2**
Title:	**POPD – Requirement No. 2**
Lead beneficiary:	**INSP**
Work package:	WP7
Dissemination level:	CO
Type	R
Due date:	31.05.2019
Submission date:	30.04.2019

Authors: **Stela Shiroka,** INSP

Yung Shin Van Der Sype, TLX

Contributors: **Peter Leitner,** INSP

Reviewers: **Yung Shin Van Der Sype,** TLX

Acknowledgement: This project has received funding from the European Union's Horizon 2020 Research and Innovation Action under Grant Agreement No 826497.

Disclaimer: The content of this publication is the sole responsibility of the authors, and does not in any way represent the view of the European Commission or its services.

TABLE OF CONTENT

EXECUTIVE SUMMARY

D7.2 ‘POPD – Requirement No. 2’ is the second WP7. ‘Ethics requirements’ deliverable in the SecureHospitals.eu project.

The goal of this deliverable is to detail how the consortium will address the POPD-Requirement of the ‘Horizon 2020 Guidance – How to complete your ethics self-assessment’, relating to the processing of personal data.

1 Introduction

D7.2 'POPD – Requirement No. 2' is the second WP7. 'Ethics requirements' deliverable in the SecureHospitals.eu project.

Instituting proper procedures for personal data handling from the project research, training and awareness raising activities is of core importance for the SecureHospitals.eu action. The project actively involves different types of healthcare and cybersecurity professionals for the purposes training, awareness raising, and engagement in mutual collaboration.

The goal of this deliverable is to detail how the consortium will address the POPD-Requirement of the 'Horizon 2020 Guidance – How to complete your ethics self-assessment'[1], with a particular focus on compliance with the data minimisation principle (cfr. Description of Action).

SecureHospitals.eu is required to confirm to process personal data in compliance with the EU principles on data protection and to set out how the data intended to be processed are relevant and limited to the purposes of the research project.

The reasoning behind this deliverable is to improve the management and monitoring of the ethics requirements throughout the lifetime of the project, in particular for the data collection during the stakeholder engagement and mobilisation activities (WP2. 'Involve' and WP3. 'Aggregate'), the launch and further development of the Open Awareness and Information Hub (WP2. 'Involve'), the research activities planned in WP4. 'Create', the training activities planned in WP5. 'Boost', and the dissemination activities under WP6. 'Communicate'.

This deliverable should be read in line with D7.1 'H – Requirement No. 1' and D1.2 'Data Management Plan'.

[1] Horizon 2020 Guidance – How to complete your ethics self-assessment, v6.1, 4 February 2019, http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf.

2 Preliminary statement

The SecureHospitals.eu research requires the processing of personal data of research and training participants and prospective research and training participants.

SecureHospitals.eu does not require the processing of special categories of personal data, including genetic, biometric and health data, nor does it require profiling, systematic monitoring of individuals or processing of large scale of special categories of data, nor the use of intrusive methods of data processing.

The research does not involve further processing of previously collected personal data. While previously collected research data are processed, these data will not include any personal data (except for the names of the authors of published research).

SecureHospitals.eu will in principle not import or export personal data. However, an American third-party service provider is engaged in order to efficiently and securely inform the stakeholders of the SecureHospitals.eu project (newsletter) and the transfer of data in this regard is covered by the EU-US Privacy Shield.

For the identification of stakeholders publicly available data will be used to the extent that such information is legally available to the consortium.

SecureHospitals.eu acknowledges that research ethics is given high priority in Horizon 2020-funded research. The consortium will hence comply with applicable national, EU and international legislation on the protection of personal data, as set out in the Description of Action and the Grant Agreement.

In particular, the consortium will aim to comply with:

- Articles 7 and 8 of the EU Charter,
- Article 8 of the European Convention on Human Rights,
- Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (CM/Inf(2018)15-final),
- Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR), and
- Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive).

In order to give body to the principles and requirements set out in the legislation above, the consortium also considers especially:

- European Union Agency for Fundamental Rights and Council of Europe, European Court of Human Rights and European Data Protection Supervisor, Handbook on European data protection law (2018 edition),
- Article 29 Working Party, Guidelines on consent under Regulation 2016/679 (WP259rev.01),
- Article 29 Working Party, Guidelines on transparency under Regulation 2016/679 (WP260rev.01), and
- All other relevant opinions and guidelines of relevant authorities, such as the European Data Protection Board and national supervisory authorities.

3 Processing of personal data in SecureHospitals.eu

3.1 Processing activities

The SecureHospitals.eu project processes personal data in the context of the following activities:

- Collection of contact information for the purposes of stakeholder engagement and mobilisation in a pan-European knowledge exchange and for further awareness raising activities,
- Research activities via an online survey to understand the general perceptions of healthcare professionals on cybersecurity,
- Qualitative trainer interviews to understand the strengths, weaknesses and potentials of current training approaches on cybersecurity in the healthcare sector,
- Various training activities in the form of a Massive Open Online Course (MOOC), a summer school, and several local workshops and webinars for healthcare professionals with different levels of knowledge on the cybersecurity topic.

3.2 Categories of data subjects

In SecureHospitals.eu personal data will be processed of the following data subjects:

- Project stakeholders,
- Research and training participants, and
- Prospective stakeholders and research and training participants.

These data subjects will be 1) healthcare professionals, such as doctors, nurses, caregivers, administrative healthcare staff handling personal data, IT staff of healthcare facilities, data protection officers of healthcare facilities, or 2) cybersecurity professionals active as trainers, solution providers, advisors, etc.

SecureHospitals.eu is committed to not process personal data of vulnerable groups of individuals, such as children.

3.3 Purposes of processing

Personal data will be processed only as part of the research inquiry of the project and within the scope of the personal data and processing of personal data definitions as set out in the Description of Action. Hence, SecureHospitals.eu will collect and process personal data from participants in the research, training and awareness raising activities and solutions.

Collection of personal data is aimed at conducting empirical research and is collected in three stages during the action:

I. Research stage (diagnostic and explorative data): This stage includes the processing of personal data in the context of a survey with different stakeholders, interviews with cybersecurity trainers and potentially with other types of stakeholders (e.g. researchers,

decision- and policy-maker) in order to explore their views on the challenges, trends, remedies and potentials of cybersecurity in the healthcare sector,

II. Training and awareness raising stage (process-oriented data): This stage will include the processing of personal data as a consequence of registrations to the project newsletter, registrations on the SecureHospitals.eu Open Awareness and Information Hub, registrations to the Massive Open Online Course, and participation to consortium events by sharing photo and video footage,

III. Training assessment stage (evaluative data): This stage will include the processing of personal data for reviewing the participant evaluations forms for the trainings conducted by the consortium as well as for issuing certificates to participants who complete the courses (MOOC and summer school).

3.4 Legal grounds for processing

In principle, all processing activities in the SecureHospitals.eu project will be based on the consent of the data subject. Participants and stakeholders will be asked to consent to the processing of their personal data for the participation in the research studies and trainings. Interested stakeholders will be asked to opt-in to receive project communications (newsletter). Consent will be informed and will be asked for each purpose and for each activity separately. Therefore, for example, training participants will be asked for a separate consent to process their personal data in the context of the evaluation sheets, separately from the trainings.

For identifying prospective stakeholders online based on publicly available data, the legal ground for processing will be the legitimate interest of SecureHospitals.eu, namely, to conduct its research activities and to reach out to a large and diverse pool of potential stakeholders.

4 Data protection safeguards

4.1 Background

The consortium has assessed the requirement to address privacy and data protection issues prior to conducting any research studies or trainings and even prior to the start of the project. Section 6 'Ethics and security' of the Description of Action sets out the basic principles that will be followed by SecureHospitals.eu.

During the first months of the project the consortium has re-assessed and further specified certain aspects of the commitments set out in the Description of Action.

As a result, the consortium confirms its commitment to comply with the principles and requirements of EU data protection law.

Moreover, the consortium still holds the opinion that the appointment of a formal DPO is not required on a project-level. Firstly, one of the project partners (TLX) was in particular involved in the project for its expertise on privacy and data protection matters. Secondly, most partners are by themselves obliged to appoint a DPO for their organisation and the activities of the project are in line with the daily business of these organisations.

In the context of the re-assessment of the project's legal commitments, it has been further specified how to comply with the data minimisation principle, were several agreements concluded and procedures implemented, and were additional safeguards discussed based on the e-Privacy Directive. These measures are reported below.

4.2 Data minimisation

The collection and processing of personal data in SecureHospitals.eu will be carried out in compliance with the data minimisation principle. As a basic rule, personal data will be processed only when strictly necessary to achieve the defined project objectives and key performance indicators as set out in the Description of Action. While researchers tend in general to collect more personal data than necessary for the study on a 'you never know'-basis, SecureHospitals.eu is actively going against this over-collection approach not only for the protection of personal data, but also because the project believes that pre-defined and clear research scopes and methods lead to more relevant and accurate research results.

To this end, the processing of personal data will be limited at the earliest stages of the processing activities, *i.e.* at the time of the collection of the data, either by the intention to collect only anonymised research data or by pseudonymising personal data of participants. Participants of research activities including the survey, interviews and training evaluation forms will not be required to mention their name, affiliation or other information that makes them directly identifiable. Nonetheless, the consortium is cautious for the processing of indirectly identifiable data. Pseudonymisation techniques are applied to research data collected, dividing the content data from its direct identifiers (if any) so that linkage to a person is only possible with additional information that is held securely and separately. In order to analyse the research results and to compare the

responses of different participants, a participant number will be assigned to the responses of each participant.

The participant responses will be analysed by the consortium and only aggregated research data will be used for scientific publications and presentations at conferences, workshops and other dissemination purposes.

Personal data will not be shared with or disclosed to third parties, external to the consortium, except in cases where the consortium relies on third-party service providers, e.g. for hosting the website or to manage the project communication (cfr. *Infra*).

The personal data of research participants will be retained during the lifetime of the project. After the end of the project, the raw research data will be deleted as soon as is contractually allowed, considering the retention requirements for research funded by the European Commission.

4.3 Procedural commitments

In order to safeguard the transparency of the processing activities, the data subjects are informed about the processing activities by the **project's data protection notice**. The project's data protection notice is available on the project website and will also be integrated in the Open Awareness and Information Hub (to be developed as part of WP2). All online study and survey participants and all participants to face-to-face interviews and trainings will be informed about the processing of their personal data before their actual participation.

Informed consent of data subjects is asked as described in D7.1 'H – Requirement No. 1'. Reference to the data protection notice is made in order to obtain *informed* consent of the data subjects.

In order to divide the responsibilities between the project partners for the processing of personal data, the partners have concluded a **controller-to-controller agreement**, which, for example, clarifies the roles of the different partners, confirms the confidentiality of the personal data, and requires partners to ensure the security of the personal data also on a partner-level. The latter is important, as personal data will be collected at different research sites, and while on project-level, state of the art technologies and methods are applied for the secure access, storage and transfer of personal data, all partners had to ensure that the collected data will – on their sites, also – be stored on a secure server and will be only accessible by their authorised personnel. Another important aspect of the controller-to-controller agreement is also the cooperation mechanism that is put in place between the partners, requiring them to cooperate with each other in the event of a data breach or for addressing data subject rights requests.

Given that the project is responsible for any partners, contractors or service providers that process research data at the project's request on the project's behalf, the project coordinator (INSP) has executed **data processing agreements** with third-party services providers that are engaged in specific tasks of the project (such as sending the newsletter and hosting the database).

Where service providers from outside the European Economic Area would be engaged and personal data would be transferred to a country outside of the European Economic Area, the adequate level of protection of the personal data abroad will be ensured either by choosing a service provider based in an 'adequacy decision'-territory or in accordance with the **standard contractual clauses** for data

transfers. At this point, personal data are only transferred outside the European Economic Area to one service provider that is trusted with the administration of the newsletter (covered by the **EU-US Privacy Shield**).

4.4 Additional safeguards

Finally, it should be pointed out the consortium also complies with the requirements of the e-Privacy Directive, which aims at the protection of personal data in the electronic communications sector. It addresses the confidentiality of information, treatment of traffic data, spam and cookies. Compliance with the e-Privacy Directive is essential for SecureHospitals.eu for the provision of the website and the web platform.

Another element of the Directive relates to the passing on of e-mail addresses to third parties (e.g. marketing companies) and the case of unsolicited e-mails (spam) unless recipients have agreed to receive such emails (e.g. newsletters or e-mail lists).

The directive also requires websites to get consent from visitors to store or retrieve any information on a computer, smartphone or tablet with cookies. Through the implementation of cookies users are more aware of how their information is collected and used while they visit a website. The users also have the choice to allow this information to be collected or not. To explain the use of cookies by SecureHospitals.eu a **cookie policy** is available on the project website.

5 Conclusion

The SecureHospitals.eu project research requires the processing of personal data of stakeholders, participants and prospective participants.

Data subjects are informed about the processing of their personal data and about the legal bases thereof. The consortium partners have executed a data exchange agreement amongst the partners in order to divide the responsibilities of processing and to define the minimum requirement each partner needs to ensure. In addition, website visitors and platforms users are (or will be) informed about the use of cookies, etc. and stakeholders will only receive project communication after actively subscribing to the newsletter.

6 References

Websites:

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