**WP 2 – Responsible innovation: Ethical, Legal and Societal Aspects**

***Workshop - Questionnaire***

|  |  |
| --- | --- |
| ****Project number**** | **830892** |
| ****Project acronym**** | **SPARTA** |
| ****Project title**** | **Strategic programs for advanced research and technology in Europe** |
| ****Start date of the project**** | **1st February, 2019** |
| ****Duration**** | **36 months** |
| ****Programme**** | **H2020-SU-ICT-2018-2020** |

**Editor**

Jean-Marc Van Gyseghem, Manon Knockaert (UNamur)

**Contributors** (ordered according to beneficiary numbers)

**Reviewers** (ordered according to beneficiary numbers)

**Disclaimer**

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

Table of Contents

[I. Objective 3](#_Toc16064368)

[II. General questions 3](#_Toc16064369)

[III. Thematic questions 4](#_Toc16064370)

[1.1 Program #1: T\_SHARK – Full spectrum cybersecurity awareness 4](#_Toc16064371)

[1.1.1 Description 4](#_Toc16064372)

[1.1.2 Data Management 4](#_Toc16064373)

[1.1.3 Questions 4](#_Toc16064374)

[1.2 Program #2: CAPE – Continuous assessment in polymorphous environments 5](#_Toc16064375)

[1.2.1 Description 5](#_Toc16064376)

[1.2.2 Data management 5](#_Toc16064377)

[1.2.3 Questions 5](#_Toc16064378)

[1.3 Program #3: HAIIT- High Assurance Intelligent Infrastructure Toolkit 6](#_Toc16064379)

[1.3.1 Description 6](#_Toc16064380)

[1.3.2 Data management 6](#_Toc16064381)

[1.3.3 Questions 6](#_Toc16064382)

[1.4 Program #4: SAFAIR – Secure and Reliable AI Systems for Citizen 7](#_Toc16064383)

[1.4.1 Description 7](#_Toc16064384)

[1.4.2 Data management 7](#_Toc16064385)

[1.4.3 Questions 7](#_Toc16064386)

1. Objective

The objective of this questionnaire is to be a working basis to facilitate the discussions during the ethical and legal workshop organized during the Sparta Days (24-25 September 2019).

The results of the questionnaire will make it possible to support the analysis of literature by the contributions of the field and practice to the identification and description of issues.

The results will be analysed and integrated into the deliverable D2.1-Ethical, legal and societal aspects. The objective is the provision of a documented list of relevant ethical, legal and societal aspects relevant in the context of large-scale cybersecurity research and innovation.

1. General questions

* Should we give more information to the data subject in order to ensure a transparent processing and to obtain his/her consent than what is required by the GDPR?
* How to reinforce the right to be informed in the context of cybersecurity and innovation?
* What information should be given to the data subject to understand the system’s functioning in order to guarantee a real right to contest to the data subject?
* What are the major obstacles in the collection of personal data to avoid algorithmic bias? What constitutes a real alternative able to guarantee the free aspect of a consent given by the data subject?
* How can we address the challenge to manage access to the personal data and individual privacy?
* Does the right to the portability of personal data imply interoperability? If so, how can it be exercised in a cybersecurity context? If not, should it be made mandatory?
* Should the notion of privacy by default and by design involve regular updates?
* Has the empowerment of citizens promoted by the GDPR leading to more responsibility for the data subject?
* How can we ensure the right to erasure with the need to obtain more personal data to verify the subject’s identity?
* Is the right to data portability - which is the possibility for the data subject to receive his/her personal data and provided it to another data controller - enough to avoid dependency effect?
* How to deal with the new forms of dilution of responsibility (e.g. the creator of the algorithm, the user, the provider of the devices) implied by complex and highly segmented algorithmic systems?
* Do you face challenges or difficulties with the use of personal data?

1. Thematic questions

## Program #1: T\_SHARK – Full spectrum cybersecurity awareness

### Description

Evolving cyber-threats varying in scope, scale, duration, intensity, complexity, sophistication and impact, are getting increasingly common and demand a mobilization of the full range of respective tools and instruments, as well as a joint response. A collective cross-sectorial and wide-ranging approach, providing comprehensive situational threat intelligence, enabling future prediction, and informed and effective decision-making, is indispensable to address a widening and deepening landscape of hazards raging. Much of the current organization of cybersecurity supervision is organized as a reactive activity, focusing on individual incident handling, driven by technology aspects, resulting in limited abilities to spot on early stage new generation threats. To reach catch up with evolving cybersecurity threats, these practices should evolve to more comprehensive, wider spectrum, prediction based, cognitive computing capabilities. The objective of this WP is to develop and validate methodological, organizational and technological solutions extending cybersecurity towards comprehensive organization of security functions, that would focus more on threat prediction and full-spectrum cybersecurity awareness, providing high situational awareness, informing decision and policy makers on broad or long-term issues and/or providing a timely warning of threats. It will expand the reach of threat understanding, from current investigative-level definition, up to strategic considerations on current, future and down to real-time events handling and prevention. The T-SHARK Program addresses four challenges: the first is to handle complex of cybersecurity threats (T4.2, T4.3). The second deals with early cyber attacks’ kill chain phases (T4.2). The third aims at developing methods and solutions for prediction and awareness- and knowledge-based cybersecurity management (T4.3, T4.4) . The fourth focusses in the exchange of Threat Intelligence information between sharing partners and the actionability on such data regarding the GDPR (T.4.5). Activities will be performed cross-vertical, cross-domain to assure comprehensiveness aspect of the challenges addressed, and demonstrated over use cases (T4.1, T4.6).

### Data Management

* ***Do you process[[1]](#footnote-1) personal data[[2]](#footnote-2)?***

***If yes,***

***please provide with the more examples as possible***

* ***Do you process special categories of personal data (e.g. biometrics data, genetic data, health data, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, judicial data?)***

***If yes,***

***please provide with the more examples as possible***

### Questions

***To be completed by the partners***

## Program #2: CAPE – Continuous assessment in polymorphous environments

### Description

Assessment is difficult for two main reasons, access and pace of change. With respect to access, the complexity of current developments makes in-depth holistic understanding of the source of some of the fundamental IT technologies, for example hardware or operating systems, completely out of reach to anyone but their developers. With respect to pace, digital technologies are being introduced and deeply woven into new or existing systems and services, providing benefits such as energy efficiency, but also introducing new vulnerabilities and thus new risks as they are updated and reconfigured. Without the capability for assessments of tools and services, risk assessment and thus suitability are increasingly difficult, to the point of being economically impractical or technically impossible. The CAPE Program focuses on providing practical tools to product and service developers, in the following key areas. First, it addresses the definition of assessment targets, including in the scope differential assessment. Second, it includes in assessment the creation and validation of proper audit trails for intrusion detection, impact assessment and forensics. It also includes in its scope the capability to go beyond assessments of components and products, but also complex services, to take into account a more comprehensive component-based approach. Finally, it links with the training program to ensure that certified components and services are properly developed and operated. The CAPE Program addresses five challenges: the first one aims at developing more agile assessment and certification frameworks, similar to agile development (T5.1, T5.2). The second aims at automation, supporting developers in writing requirements and executing tests (T5.1). The third challenge deals with assessing systems of systems, beyond individual components, and modularizing assessment to enable assessment of complex systems and services (T5.3). The fourth challenge addresses lifetime dynamicity of environments who may have long lifespans, but where individual components might be replaced or upgraded (T5.2, T5.3). Finally, the fifth challenge addresses execution elasticity, particularly for services (T5.3). These challenges are demonstrated over three use cases (T5.4).

### Data management

* ***Do you process[[3]](#footnote-3) personal data[[4]](#footnote-4)?***

***If yes,***

***please provide with the more examples as possible***

* ***Do you process special categories of personal data (e.g. biometrics data, genetic data, health data, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, judicial data?)***

***If yes,***

***please provide with the more examples as possible***

### Questions

***To be completed by the partners***

## Program #3: HAIIT- High Assurance Intelligent Infrastructure Toolkit

### Description

IoT-connected devices bring immense promise for industry and society as a whole, as they evolve towards a true Intelligent Infrastructure (II). But along with opportunities they also bring new points of vulnerability that enable attackers to steal or affect sensitive data or control devices remotely. Indeed state-of-the art security mechanisms are rarely adaptable to IoT devices and overall security guarantees are hard to obtain. In this context security is hard to develop, as witnessed IoT components that have been proposed, only to be broken soon after. Considering security and resilience requirements in future II systems from the outset (rather than being an add-on) is thus of paramount importance and providing practical tools to achieve this is the objective of the HAII-T Program. To this end we will develop a secure-by-design development framework and a toolkit supporting the design, development and verification of security-critical, large-scale distributed II systems. The framework will support the specification and enforcement of key security policies including the confidentiality, integrity, resilience and privacy of the exchanged data. The challenge will be addressed jointly through secure system software (T6.1), hardened legacy components (T6.2), secure orchestration of II components (T6.3), building in resilience (T6.4) and auditable data privacy protection (T6.5).

### Data management

* ***Do you process[[5]](#footnote-5) personal data[[6]](#footnote-6)?***

***If yes,***

***please provide with the more examples as possible***

* ***Do you process special categories of personal data (e.g. biometrics data, genetic data, health data, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, judicial data?)***

***If yes,***

***please provide with the more examples as possible***

### Questions

* It is important that, in the use of cloud computing services, the data controller keep the control over the client of cloud computing services. What mandatory obligations should be given by the data controller? How can we avoid a gap in the possibility of negotiation for SMEs?
* Is the use of US cloud services a security risk?
* How can we prevent connected objects from becoming spy objects?
* How can we always guarantee the trust of users of connected objects while ensuring that they are aware of the potential risks?
* What are the main ethical challenges regarding IoT devices?
* How to manage the right to privacy and the right to be left alone with IoT connected devices?

## Program #4: SAFAIR – Secure and Reliable AI Systems for Citizen

### Description

Currently we face two major problems with regards to AI systems: the first, technical one, with regards to lack of understanding of the scope of cybersecurity issues and solutions in the light of new complex cyberattacks, and second (technical and SSH) with regards to trust, fairness, legal and social challenges as well as explainability aspects of such systems. We believe that SPARTA’s SAFAIR Program will address the abovementioned aspects. The main objective of this Program is to ensure trustworthiness of Artificial Intelligence (AI) systems, including security, privacy and reliability. The work package will produce formalisms, methods and tools to make AI-based systems more robust to attackers' manipulation, allowing to assess fairness of AI algorithms, extending explainability of results. Furthermore, the goal is to make AI systems more reliable and resilient through enhanced explainability and better understanding of threats. In summary, the Program aims to address 5 challenges. First, to design and develop threat analysis supporting tools for AI systems, in order to make them more understandable by both developers and users (T7.1). Then to design and develop defensive and reactive security mechanisms that make AI systems more security- and privacy-aware and ensure resilience against the identified threats (T7.2). A third challenge is to design and develop methods to increase AI systems reliability and resilience through enhanced explainability of the functioning (T7.3). Challenge four is ensuring the fairness of AI systems by providing mechanisms to reduce bias in the decisions based on AI systems need and ensure accountability and correct compliance with EU regulations, privacy aspects and data protection including compliance with GDPR (T7.4). These challenges and explored solutions will be illustrated by demonstration cases (T7.5) validating the scope of the issue and the efficiency of all the methods and tools implemented on reliable AI.

### Data management

* ***Do you process[[7]](#footnote-7) personal data[[8]](#footnote-8)?***

***If yes,***

***please provide with the more examples as possible***

* ***Do you process special categories of personal data (e.g. biometrics data, genetic data, health data, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, judicial data?)***

***If yes,***

***please provide with the more examples as possible***

### Questions

* What positive contributions AI technologies should have on current societal challenges regarding cybersecurity (for examples in specific areas such as health, transportation, energy efficiency)?
* Should we ensure the possibility to always have a human intervention during the processing of personal data by algorithms?
* What are the risks to have a real automatic decision by the machine?
* In the use of artificial intelligence techniques, who should be responsible in case of harm or damages (e.g. the creator of the algorithm, the user, the provider of the devices? What should be the criteria in order to determine the responsibility?
* How should we manage the minimization and proportionality principles set by the GDPR with the need to have the most data as possible “to feed” and design efficient algorithms in order to avoid bias?
* Is there any risk of non-democratisation of artificial intelligence tools for cybersecurity that will reinforce the gap between big and smaller firms?
* How can we avoid blackboxes’ phenomenon? Is the legal constraint to make the automatic decisions understandable enough?
* How to ensure that AI developments serve citizens?

1. Processing = Any operation or set of operations which is performed on personal data or on sets of personal data (e.g. 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). [↑](#footnote-ref-1)
2. Personal data = Any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly by, for example, a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. [↑](#footnote-ref-2)
3. Processing = Any operation or set of operations which is performed on personal data or on sets of personal data (e.g. 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). [↑](#footnote-ref-3)
4. Personal data = Any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly by, for example, a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. [↑](#footnote-ref-4)
5. Processing = Any operation or set of operations which is performed on personal data or on sets of personal data (e.g. 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). [↑](#footnote-ref-5)
6. Personal data = Any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly by, for example, a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. [↑](#footnote-ref-6)
7. Processing = Any operation or set of operations which is performed on personal data or on sets of personal data (e.g. 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). [↑](#footnote-ref-7)
8. Personal data = Any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly by, for example, a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. [↑](#footnote-ref-8)