a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services

D2.6 - SPIDER Ethical, Privacy and Legal Requirements - Final Version

Grant Agreement number:	833685
Project acronym:	SPIDER
Project title:	a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services
Start date of the project:	01/07/2019
Duration of the project:	36 months
Type of Action:	Innovation Action (IA)
Project Coordinator:	Name: Pier Luigi Polvanesi Phone: +39 010 600 2662 e-mail: pierluigi.polvanesi@ericsson.com

Due Date of Delivery:	30/06/2020
Actual Date of Delivery:	02/07/2020
Work Package:	WP2 - Requirements Analysis, Architecture Definition and Pilot Use Cases
Type of the Deliverable:	R - Report
Dissemination level:	P - Public
Main Editors:	CLS
Version:	V1.0

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685.

List of Authors, Contributors, Reviewers

Name	Role	Organization
Eirini Karapistoli Matthias Ghering George Alexopoulos	Author	CYBERLENS LTD
Panagiotis Gouvas Anastasios Zafeiropoulos	Contributor	GIOUMPITEK MELETI SCHEDIASMOS YLOPOIISI KAI POLISI ERGON PLIROFORIKIS ETAIREIA PERIORISMENIS EFTHYNIS
Anna Angelogianni Christos Xenakis	Contributor	UNICERSITY OF PIRAEUS
Yiannis Tsampoulatidis	Reviewer	INFALIA PRIVATE COMPANY
Maurizio Giribaldi Guerino Lamanna	Contributor	INFOCOM S.R.L.
Maria Crociani	Reviewer	SPHYNX TECHNOLOGY SOLUTIONS AG

History of changes

Version	Date	Change History	Authors	Organization
0.1	31/03/2020	Initial version	Irene Karapistoli, Matthias Ghering, George Alexopoulos	CLS
0.2	03/04/2020	Updated ToC	Irene Karapistoli, Matthias Ghering, George Alexopoulos	CLS
0.3	08/04/20	Updated version. Contributions added to Section 7.1	Irene Karapistoli, Matthias Ghering, George Alexopoulos	CLS
0.4	15/05/20	Updated version. Contributions to Section 7.2	Irene Karapistoli, Matthias Ghering, George Alexopoulos	CLS
0.5	29/05/2020	Further work to submit document for internal review	Irene Karapistoli, Matthias Ghering, George Alexopoulos	CLS
0.6	08/06/2020	Revised version after contributions from UBI and INFO.	Irene Karapistoli, Matthias Ghering, George Alexopoulos	CLS
0.7	12/06/2020	Cleaned-up version submitted for internal review	Irene Karapistoli, Matthias Ghering, George Alexopoulos	CLS
0.8	23/06/2020	Revised version following the comments from INF and STS.	Irene Karapistoli, Matthias Ghering, George Alexopoulos	CLS
0.9	01/07/2020	Revised version following the comments from the Ethics Advisory Board	Irene Karapistoli	CLS
1.0	02/07/2020	Document ready for submission to the European Commission	Irene Karapistoli	CLS

Glossary

Acronym	Explanation
CFR	Chapter of Fundamental Rights
CoE	Council of Europe
CRaaS	Cyber Range as a Service
DMP	Data Management Plan
DoA	Description of the Action
DMP	Data Management Plan
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
EU	European Union
GA	Grant Agreement
GDPR	General Data Protection Regulation
H2020	Horizon 2020
PICF	Participant Information and Consent Form
PII	Personal Identifiable Information
POPD	Protection of Personal Data
PUC	Pilot Use Case
WP	Work Package

Disclaimer

The information, documentation and figures available in this deliverable are written by the SPIDER Consortium partners under EC co-financing (Call: H2020-SU-DS-2018, Project ID: 833685) and do not necessarily reflect the view of the European Commission.

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 reader uses the information at his/her sole risk and liability.

Table of Contents

List of Tables

List of Figures

Executive Summary

Deliverable D2.6 “SPIDER Ethical, Privacy and Legal Requirements – final version” reports the ethical, privacy and legal requirements of the SPIDER project and platform. This document describes the ethical, privacy and legal considerations as well as the respective procedures that are in place at a European and national level to ensure that the SPIDER project remains compliant with the applicable laws. It also provides guidelines and answers to ethical, privacy, data protection and legal issues as well as on the technical approach the SPIDER platform will adopt for the relevant ethical issues specifically for the human involvement.

The ethics guidelines will be primarily applied to the management and execution of the SPIDER pilots (WP7 - Demonstration and Evaluation). However, ethics and data protection legislation, guidelines and principles have to be followed much earlier, during the user requirements elicitation phase (WP2 - Requirements Analysis, Architecture Definition and Pilot Use Cases, Task 2.1 - Analysis of User and Cybersecurity Requirements), as well as when dealing with workshop arrangements and similar dissemination and communication activities.

The ethical, privacy and legal guidelines and the outcome of this deliverable will guide the pilot-related activities of the SPIDER project and will be used as input to Task 2.3 “Platform Architecture and Specifications”, assisting in the definition of the SPIDER platform architecture.

While this final version of the document contains a complete and thorough description of the ethical, privacy and legal requirements of the SPIDER project, regular check points on these requirements will be performed to ensure that all ethical, privacy and legal considerations of the SPIDER project are implemented as foreseen. Should changes on the ethical, privacy and legal requirements of the SPIDER project arise, these changes will be reported in dedicated sections of the Deliverables D1.4 “Interim project report” (due to M18) and D1.6 “Final project report” (due to M36).

1 INTRODUCTION

1.1 SCOPE

SPIDER is an innovative cybersecurity project conceived to face the rapidly increasing complexity of the telecommunication domain's cyber threat landscape and its consequent requirements, namely:

- need for effective tools to improve the technical security skills of experts and non-experts in the multi-tenant and multi-service environments coming with the domain's 5th Generation (5G);
- need for highly customisable and dynamic network modelling instruments that will enable real-life virtualisation and real-time emulation of networks and systems;
- need for cyber econometric capabilities to enable customers to forecast the evolution of attacks and their associated economic impact.

SPIDER aims to deliver a next-generation, extensive, and replicable cyber range as a service (CRaaS) platform for the telecommunications domain and its fifth generation (5G), offering cybersecurity emulation, training and investment decision support. Towards this vision, it features integrated tools for cyber testing including advanced emulation tools, novel training methods based on active learning as well as econometric models based on real-time emulation of modern cyber-attacks.

This deliverable contains critical information regarding the ethical, privacy and legal requirements of the SPIDER platform. More specifically, according to the Description of Action (DoA) [1], the purpose of this document is to identify ethical issues, privacy concerns as well as legal requirements that may arise in the execution of the SPIDER project and its pilot use cases, and in particular, issues related to privacy and personal data protection, while considering aspects that are specific to each pilot country (Italy, Spain, Greece and UK) and which are generally valid at the European level.

The output of this deliverable will contribute to the discussions related to the development of the different technical components of the SPIDER platform.

1.2 AUDIENCE

The intended audience for this deliverable is preliminarily the SPIDER partners as the work contained in this document will support the implementation of the SPIDER platform and the execution of the SPIDER pilots. However, the research work regarding the European Union (EU) regulatory frameworks on privacy and protection of personal data as well as the national data protection frameworks in the SPIDER pilot countries country (Italy, Spain, Greece and UK), will be of interest to a wider audience such as policy makers, researchers, and the general public.

1.3 STRUCTURE

The remainder of the document is structured as follows:

- **Section 2** begins with an analysis of the requirements for privacy protection in the context of the SPIDER project. By relying on input from two Ethics Deliverables, namely D9.1 ("H – Requirements No. 1") and D9.8 ("POPD-Requirement No. 8"), the analysis concludes that only a subset of the General Data Protection Regulation (GDPR) is in scope of the present deliverable, this section then surveys the EU regulatory framework for privacy and protection of personal data. The relevant articles and recitals of the GDPR are outlined to facilitate the comprehension of the wider scope

of the Regulation. This section concludes with a special focus on the national legislations which are in place at the country level of the four SPIDER pilot sites (Italy, Spain, Greece and UK).

- **Section 3** discusses issues related to data security and anonymization.
- **Section 4** elaborates on the privacy protection aspects of the SPIDER platform. Particular emphasis is given to the privacy protection issues in the activities of WP2 and WP7.
- **Section 5** presents the legal and ethical framework for the involvement of human subjects in the development and testing of the SPIDER platform.
- **Section 6** elaborates on the human involvement in the SPIDER activities and the associated ethical concerns. Similar to Section 4, emphasis is given to the activities of WP2 and WP7 as well as to workshop arrangements.
- **Section 7** summarises the ethical, privacy and legal requirements of the SPIDER platform and maps them to the pilot use cases.
- **Section 8** concludes this deliverable with the outcomes of the legal analysis and with the SPIDER platform guidelines for handling ethical issues.

1.4 INTERACTIONS

Ethical issues in SPIDER will be scrutinized in close synergy with data management, pilot and legal issues activities, conducted under Task 1.4 (Data Management), WP7 (SPIDER Demonstration and Evaluation) and Task 2.2 (Analysis of Ethical, Privacy and Legal Requirements) respectively.

Ethical issues also apply for the user requirements elicitation phase associated with Task 2.1 (Analysis of User and Cybersecurity Requirements).

The interaction between the abovementioned SPIDER activities is illustrated in Figure 1.

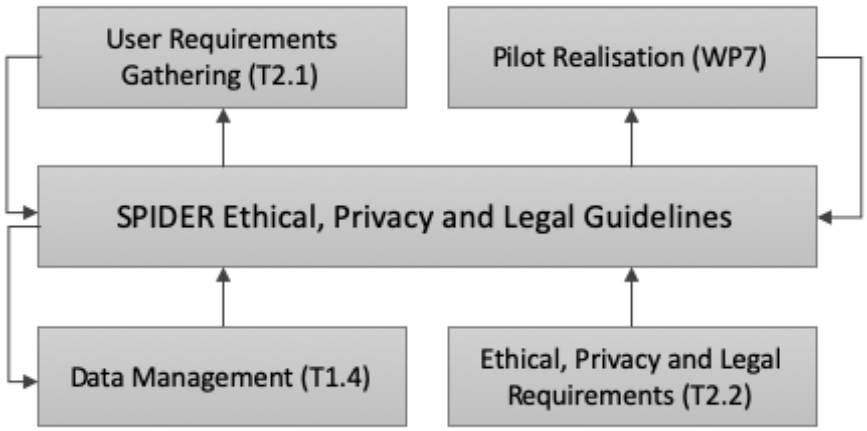

Figure 1: SPIDER ethical issues interrelations

It is worth noting here that the specific requirements for privacy and personal data protection are dealt with in two other Ethics Deliverables of WP9, namely in D9.1 (“H – Requirements No. 1”) - informed consent procedures for the participation of humans, and in D9.8 (“POPD-Requirement No. 8”) - informed consent with regard to data processing.

2 LEGAL FRAMEWORK FOR PRIVACY PROTECTION

The SPIDER project aims to develop, and pilot test a Cyber Range as a Service (CRaaS) platform, whose goal is to provide virtualised 5G cyber range services to 5G telecommunications providers and security professionals, ICT vendors, etc. In order to fulfil its objective, SPIDER must comply with the European regulations and norms related to personal data protection and privacy.

Since May 25, 2018, the collection, use and disclosure of personal data at a European level are regulated by the General Data Protection Regulation (GDPR) EU/679/2016 on protection of personal data [2]. According to Article 4.1 of GDPR, "*'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*".

Privacy protection issues typically arise in all Horizon 2020 research and innovation projects where testing and pilot execution phases exist, and the collection of information about individuals, public entities and private organizations is required. However, this is not the case for the SPIDER project. At the time of writing this deliverable and following the analysis conducted in the Ethics Deliverables D9.1 ("H – Requirements No. 1") [17] and D9.8 ("POPD-Requirement No. 8") [18], both the research and pilot activities of the SPIDER project do not deal with the collection, processing and/or storage of personal data. A detailed analysis about the SPIDER context, as presented in Sections 4 and 6 of this deliverable, has concluded that the SPIDER research activities do not present an ethics risk to the research participants due to the **absence of personal data** in all phases of the SPIDER project following the Consortium's choice to use **anonymous data collections** and **anonymous user participation in the project pilots**.

Apparently, due to the dynamic nature of the project, this is an ongoing analysis that will be updated by month 12 of the project in order to be able to reflect important changes to the project, should such changes arise. At month 12 of the project, when the final version of this deliverable will be submitted, it will reflect SPIDER's final standpoint with regard to the project's ethical, privacy protection and legal requirements.

With SPIDER not collecting, processing and/or storing personal data, it becomes apparent that only a subset of the GDPR is applicable to the project. Despite that fact, next, we review the EU legal frameworks for data protection and privacy providing a short introduction on their key principles. The provided text constitutes an overview and a brief general introduction and does not substitute the detailed obligations contained in the official regulations. Most importantly, the relevant articles and recitals of the GDPR are outlined to facilitate the comprehension of the wider scope of the Regulation.

2.1 OVERVIEW OF THE DATA PROTECTION AND PRIVACY LAWS IN EUROPE

The privacy of SPIDER's users is of paramount concern to the SPIDER consortium. Privacy is enabled by the protection of the personal data. There are several legal acts within the EU Law that address and regulate the issue of data protection. These are:

2.1.1 General Data Protection Regulation (GDPR)

The **General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR)** is a European Union (EU) law which entered into force in 2016, and became directly applicable law in all Member States of the

European Union on 25 May 2018, following a two-year transition period. The GDPR has replaced the previous Data Protection Directive (95/46/EC) [3] and its national implementations. Being a Regulation, and not a directive, GDPR does not require any EU Member State to pass any enabling legislation through national law and is directly binding and applicable. The GDPR text is available on the Eur-Lex website [2].

The GDPR lays down rules relating to the protection of natural persons with regard to the processing of personal data (Article 1), and applies to the processing of personal data (Article 2). The GDPR provisions do not apply to the processing of personal data of deceased persons or of legal entities. They do not apply either to data processed by an individual for purely personal reasons or activities carried out at home, provided there is no connection to a professional or commercial activity. When an individual uses personal data outside the personal sphere, for socio-cultural or financial activities, for example, then the data protection law must be respected. A list of key GDPR principles is summarised below.

List of key GDPR Principles:

1) The GDPR intends to protect personal data processed by legal entities. Therefore:
    a. It does not apply to personal data collected by individuals for their private use.
    b. It does not apply to data that cannot be linked to individuals. For instance, data provided by a temperature sensor fixed on a street light will not be considered as personal data (there is no link with a natural person), while the geolocation data and sensors data collected from a smart phone will be considered as a personal data, because they can be linked to a person.
2) The GDPR applies to the processing of personal data regardless of the means used, whether automated (e.g., a website, a web app, a network of sensors) or not automated (e.g., a filing system based on paper).
3) The GDPR has an extra-territorial reach, meaning that its rules apply not only to controllers or processors established in the European Union, but also to entities having their establishment in a third country, if they:
    a. Offer goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the Union; or
    b. Monitor the data subjects' behaviour, as far as their behaviour takes place within the Union.
4) Personal data cannot be processed without a legal ground or the agreement of the data subject. This usually entails that the data subject has to give his/her consent to the processing of his or her personal data for one or more specific purposes; however, different legal grounds may apply, in different instances, which could exempt controllers or processors from collecting the data subject's consent. This holds true when personal data processing:
    a. is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (e.g. when transferring connected cars' data to an external provider of maintenance services, as agreed with the car's owner through a contract);
    b. is necessary for compliance with a legal obligation to which the controller is subject (e.g. a Union, national or regional law setting out rules and obligations for cities within smart cities' programs);

c. is necessary in order to protect the vital interests of the data subject or of another natural person;

d. is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

e. is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (the discipline of the legitimate interest still vary across EU Member States and needs a case by case assessment).

5) Consent should be free, unambiguous, informed, prior and demonstrable by the data controller, meaning that it must be documented somehow (also electronically, e.g. by means of a log).

6) In any event, data subjects must be informed about the processing undergone by their personal data before the processing starts or, when data are not collected from the data subjects themselves, within a reasonable period, in any event no later than the first communication or the first disclosure to the public, when such activities are foreseen.

7) Data protection principles (i.e. data minimization, purpose limitation, data accuracy, storage limitation etc.) must always be respected; a data controller may have a legal ground to process personal data (e.g. the data subject's consent), yet it may still run the processing in breach of one of the key data protection principles, which would make the personal data processing unlawful and, potentially, trigger a sanction by competent authorities. This is the essence of the principle of accountability.

8) Risky processing for the data subjects requires a Data Protection Impact Assessment (DPIA). In particular, the DPIA shall be carried out in the case of:

a. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person (e.g. when an insurance company uses data drawn from collected cars to build customers' profiles and premiums);

b. processing on a large scale of special categories of data;

c. a systematic monitoring of a publicly accessible area on a large scale. However, it is recommended to perform a DPIA before starting any data collection from data subjects in any pilots.

9) Clear procedures must be in place to ensure data subjects' rights, namely:

a. Right of access to their data and to receive any important information on what it is done with the data;

b. Right to rectification, when the personal data are processed in a non-accurate way;

c. Right to erasure, under certain conditions, in particular when data have been processed unlawfully or are no longer necessary;

d. Right to restriction, meaning the right to "freeze" data and obtain that they are not processed for a certain period of time, for example when the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data);

e. Right to data portability;

f. Right to object.

10) Procedures to handle and notify Data Breaches to Data Protection Authorities and Data Subjects concerned must be in place.

11) Data collected on the data subject should be strictly necessary for the specific purpose previously determined by the data controller (the "data minimization" principle). Data that is unnecessary for that purpose should not be collected and stored "just in case" or because "it might be useful later". For example, if a large-scale event organizer needs generic data of people attending a concert, in order to issue tickets and organize the space in the venue, it would be not necessary and therefore disproportionate to collect information on the attendees' relatives in order to derive fine insights on the socio-economic cluster to which the attendees belong, which can then be used for targeted advertising.

12) Data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognized ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

13) The purpose for which the data were collected or further processed determines the length of time for which the data should be kept. Once the data are no longer needed, they should either be deleted or kept in anonymous form if they serve historical, statistical or scientific uses.

14) In cases of secondary processing of research and scientific data previously obtained for other research purposes can be used in so far as they are not incompatible. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations.

15) GDPR does not concern the processing of anonymous information. According to Recital (26) of the GDPR, the principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

As detailed above, the scope of application of this Regulation is about the protection of personal data**.** GDPR is very clear in the Recital (26) about the fact that anonymous information is not in the scope of this Regulation. Considering that:

- The SPIDER project gets inputs from research participants only on the basis of online interviews, training sessions and tests done under the scope of the SPIDER project (please review D9.1 ("H – Requirements No. 1") for further details);
- Such interviews, training sessions and tests are anonymous;
- No Personal Data are inherited by other Projects;
- GDPR is not applicable to anonymous information.

Yet, considering the importance of this topic in every H2020 research and innovation project, the analysis conducted and detailed on this deliverable could represent the basis for any future further analysis should any new privacy requirement arises in the SPIDER context.

2.1.2 ePrivacy Directive

The **ePrivacy Directive** (Directive 2002/58/EC on privacy and electronic communications) concerns the processing of personal data and the protection of privacy in the electronic communications sector and deals with the regulation of a number of important issues such as confidentiality of information, treatment of traffic data, spam and cookies [3].

List of Key e-Privacy Directive Principles:

1) Where the e-Privacy Directive provides for a specific rule applicable to natural and legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks, it prevails over the general rule set out by the GDPR (Principle of Specialty).
2) Electronic Communication Services and Networks must be secured through appropriate technical and organizational measures. (Security)
3) The confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, must be ensured (Confidentiality)
4) Access to, or storage of, information into the users' devices must be authorized by the users with a specific consent, unless it is "strictly necessary in order to provide a service explicitly requested by the subscriber or user" (so called "**cookie law**", Prior Consent). In other words, any website, or web app should provide clear information on its the cookies it deploys into the users' devices and collect the prior consent, where necessary.
5) Principles applicable to Traffic Data
    a. Traffic data must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication or for the purposes of processing subscriber's billing and interconnection payments (Traffic data erasure);
    b. Traffic data can be processed for marketing and/or for the provision of value-added services only upon specific consent of the user concerned (Consent for Marketing purposes);
    c. Specific information on traffic data processing and its duration must be provided (Specific Information);
    d. Traffic data must be processed only by persons under the authority of the service provider that are dedicated to the function or unit for which such data are necessary (e.g. handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value-added service – Authorization profiles).
6) Principles applicable to Location Data:
    a. Location data can be processed for the provision of value-added services only anonymously or upon specific consent of the user concerned (Consent for Location Data);
    b. Users must be given the opportunity to easily refuse such processing at each connection (Updated Consent);
    c. Location data must be processed only by persons under the authority of the service provider that are dedicated to the function or unit for which such data are necessary (Authorization profiles).

2.1.3 EU Cookie Directive

The **EU Cookie Directive (Directive 2009/136/EC of the European Parliament and of the Council)** is an amendment of the ePrivacy Directive (Directive 2002/58/EC) designed to increase consumer protection. The EU Cookie Directive requires websites to obtain informed consent from visitors before they store information on a computer or any web connected device. This is storage is mostly done by

cookies, which can then be used for tracking visitors to a site. The EU Cookie Directive covers all forms of online tracking technology (like flash objects and device fingerprinting) so it doesn't just apply to cookies.

The previous privacy legislation required websites to give users information on how they could remove or opt-out of cookies, which was commonly placed in privacy policies that went mostly unread. With the EU Cookie Directive, the user of a site will now be required to opt-in when using a website containing cookies. So, the website must block cookies, until visitors have given their informed consent to their use.

Directive 2009/136/EC on the protection of data and privacy on the web (EU Cookie Directive) could be used to protect the privacy of SPIDER's web-based communication channels. It could also serve as the basis for drafting the **Privacy and Cookie Policy** of the SPIDER website (http://spider-h2020.eu/).

The privacy policy will be accessible via the SPIDER website and in accordance with the GDPR, it will provide detailed information relating to (among other things) the transfer of data between relevant parties within the SPIDER consortium and will clearly explain to users, the SPIDER's policy and practices regarding SPIDER s collection, use and disclosure of users' personal information.

The cookie policy will also be accessible via the SPIDER website. In compliance with the data protection legislation and the EU Cookie Directive it will clearly explain to users what the cookies do; the potential consequences of allowing the cookies; and why SPIDER is using them. SPIDER will also obtain informed consent from users prior to using these cookies.

2.1.4 Charter of Fundamental Rights of the European Union

The Charter of Fundamental Rights (CFR)of the European Union (2012/C 326/02) brings together in a single document the fundamental rights protected in the EU. The Charter contains rights and freedoms under six titles: Dignity, Freedoms, Equality, Solidarity, Citizens' Rights, and Justice. Proclaimed in 2000, the Charter has become legally binding on the EU with the entry into force of the Treaty of Lisbon, in December 2009.

The rights of every individual within the EU were established at different times, in different ways and in different forms. For this reason, the EU decided to clarify things and to include them all in a single document which has been updated in the light of changes in society, social progress and scientific and technological developments.

The Charter entrenches:

- all the rights found in the case law of the Court of Justice of the EU;
- the rights and freedoms enshrined in the European Convention on Human Rights;
- other rights and principles resulting from the common constitutional traditions of EU countries
- and other international instruments.

The Charter sets out a series of individual rights and freedoms. The Charter is a very modern codification and includes 'third generation' fundamental rights, such as:

- data protection;
- guarantees on bioethics; and

- transparent administration.

Regarding the personal data protection, the articles 7 (respect for private and family life) and 8 (protection of personal data) of the Chapter state the following:

- *"everyone has the right to respect for his or her private and family life, home and communications"* (Article 7).
- "*everyone has the right to the protection of personal data concerning him or her*", and that processing of such data must be "*fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law*" (Article 8).

2.1.5 Council Framework Decision

Council Framework Decision (2005/222/JHA) of November 2008 addresses the most significant forms of criminal activity against information systems, such as hacking, viruses and denial of service attacks. This Decision Framework seeks to approximate criminal law across the EU to ensure that Europe's law enforcement and judicial authorities can act against this form of crime. Now, there is a proposal for a Directive on attacks against information systems, repealing Framework Decision 2005/222/JHA. Until that time, the Framework Decision 2005/222/JHA could be used in SPIDER to address confidentiality, integrity, authentication and non-repudiation features of the platform.

2.1.6 Council of Europe Convention

Council of Europe Convention 108, Recommendation R(87)15 of the Committee of Ministers of the Council of Europe on the use of personal data in the police sector, Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling.

2.2 NATIONAL FRAMEWORKS

As a 'Regulation' (and unlike the Data Protection Directive 95/46/EC that GDPR replaced), it is directly applicable and has consistent effect in all Member States of the European Union. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Since, SPIDER envisages demonstrating its research and innovation outcomes in four pilot sites in four different EU countries, namely Italy, Spain, Greece and UK, in order to get a clear and comprehensive picture of the data protection requirements, the SPIDER consortium took action and reviewed the legislation situation in the pilot countries. Next, we present a partial listing of national frameworks, national data protection laws, unfair competition legislation, telecommunications laws and any other local data protection regulations in the pilot countries involved in the SPIDER project.

❖ **Italy**

- The Italian Council of Ministers, on Aug. 8 2018, approved the **Legislative Decree n. 101/2018** harmonizing the Italian "**Privacy Code**" (D.Lgs. n. 196/2003) and other national laws with the European GDPR Regulation. The decree entered into force on 19 September 2018, and it amended a number of provisions of the Legislative Decree 196/2003. The

decree has made use of the margin of manoeuvre afforded by the GDPR to Member States as regards, in particular, processing activities based on legal obligations or for purposes in the public interest (Article 6(1), letters c) and e)); processing of biometric, genetic and health-related data (Article 9(4) and Article 36(5)); processing activities covered by Chapter IX of the GDPR (journalism, labour, research, archiving, etc.). As a result, several provisions of the Privacy Code were left in place since they did not conflict or overlap with the GDPR and provided additional value for the relevant stakeholders.

- **Legislative Decree 65/2018** implements EU Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the EU.

❖ **Spain**

- On 7 December 2018, the Spanish Senate approved the new Spanish Fundamental Law on the Protection of Personal Data and the Guarantee of Digital Rights ("**LOPD**") also known as Law 3/2018. The majority of the Organic Law 15/1999 and all legal precepts of the royal decree 1720/2007 conflicting the GDPR have been repealed [11], [12].
- The LOPD has two objectives. First, it incorporates the GDPR regulations in the Spanish legal system and provides further specifications and restrictions of its rules as explained in the GDPR. This entails that the fundamental right to data protection of natural persons, under Article 18.4 of the Spanish Constitution, shall be exercised under the GDPR and this law. Secondly, the LOPD guarantees the digital rights of citizens and employees, as specified in Article 18.4 of the Spanish Constitution. This means that it provides additional protections beyond the requirements of the GDPR regulations. For example, the LOPD includes provisions for personal data of deceased persons, the right to internet access, the right to digital education, the right to correction on the internet and the right to digital disconnection in the workplace.
- In addition to the LOPD, gross privacy non-disclosure violations might be prosecuted under criminal charges in accordance with Art. 197 of the Criminal Code.

❖ **Greece**

- In Greece, a bill of law 4624/2019 was passed on Aug 27 by the Greek parliament [13]. It should be noted that such law provides for both the legal measures implementing the Regulation 2016/679 (GDPR) in Greece, as well as the integration into the Greek legal order Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data [14].
- **Law 205/2013** on the other hand, concentrated around the protection of the integrity and availability of the services and data offered by Greek telecommunication companies. The law forces these and other related companies to build, deploy and test appropriate business continuity plans and redundant infrastructures.

❖ **UK**

- The GDPR came into force in the United Kingdom on 25 May 2018, on which date UK continues to be a Member State of the European Union.
- Alongside the GDPR, UK has prepared a new national data protection law, the **Data Protection Act 2018 ("DPA")**, which also came into force on 25 May 2018. As well as containing derogations and exemptions from the position under the GDPR in certain permitted areas, the DPA also does the following [16]:

- It allows for the continued application of the GDPR in UK national law once the UK leaves the European Union (expected to be 29 March 2019);
- Part 3 of the DPA transposes the Law Enforcement Directive ((EU) 2016/680) into UK law, creating a data protection regime specifically for law enforcement personal data processing;
- Part 4 of the DPA updates the data protection regime for national security processing; and
- Parts 5 and 6 set out the scope of the Information Commissioner's mandate and her enforcement powers and creates a number of criminal offences relating to personal data processing.

3 DATA SECURITY

Data security is a fundamental right, protected not only by national legislation, but also by European Union laws. The GDPR legislation requires that all E.U. members adopt national regulations to standardise the protection of data privacy of all citizens throughout the E.U.

The safety of the data of the SPIDER users is a fundamental design goal of the SPIDER consortium. Protecting sensitive data is the end goal of almost all IT security measures. Two strong arguments for protecting sensitive data are to avoid identity theft and to protect privacy. A good starting point when designing security controls is the C.I.A. triangle [5].

- **Confidentiality** ensures that information is not made available or disclosed to unauthorized individuals and entities.
- **Integrity** ensures that only authorized persons can modify the data/information, in accordance to law.
- **Availability** ensures that data/information is available, and only authorized persons can remove it, in accordance to law.

Anonymization or pseudonymization is one way to prevent violations of privacy and data protection [19]. SPIDER adopts this data security principle. As detailed in Deliverable D9.1 (“H – Requirements No. 1”), in SPIDER **only anonymous data will be collected and processed**.

Details of how we process and protect individuals' data will be set out and regularly updated in the SPIDER **Data Management Plan (DMP)** that comes as part of the Deliverable D1.3 “Data Management Plan” (due to month 06).

Because of that, no personal data will be collected in relation to a specific user. What is more, the name of the user will not be connected to other characteristics (e.g., age, sex, nationality and health condition). Accordingly, the presented information falls under the European legislation for securing personal data [2]. Therefore, the considerations presented in this section, as identified at the time of writing this deliverable, are for general purpose.

4 PRIVACY ASPECTS OF THE SPIDER PLATFORM

According to the analysis provided in the Deliverable D9.8 (“POPD-Requirement No. 8”), the SPIDER activities that require consideration of ethics aspects concerning the collection and processing of personal data are the activities related to WP2 (Requirements Analysis, Architecture Definition and Pilot Use Cases) and WP7 (Demonstration and Evaluation). Next, we review these two activities.

It is important to clarify from the very beginning that in all the research activities of the SPIDER project 1) no personal data will be processed, and 2) no real user traffic will be collected, i.e. only simulated/synthetic traffic will be used. Very limited contact information, such as email addresses from existing contacts, may be used as part of the usual dissemination and outreach activities.

4.1 PRIVACY PROTECTION ISSUES IN USER REQUIREMENTS COLLECTION

The procedure with which the project will define SPIDER's requirements as part of WP2 is to gather requirements from the relevant SPIDER stakeholders which, in turn, will specify the exact kind of user involvement. Each use case corresponds to a specific stakeholder and will be driven by a specific partner that will adopt the appropriate procedures for participation of humans.

The WP2 activities that could potentially involve personal data collection and processing as well as informed consent procedures are those related to Task 2.1 “Analysis of User and Cybersecurity Requirements”. This task has the primary goal to specify the different types of users of the SPIDER platform, considering both cyber security experts as well as non-experts, using different real users' profiles with a variety of expertise and multiple professional orientations.

In the context of T2.1, the different types of users and organizations that could benefit from the SPIDER platform solution have been identified. Five major stakeholder categories have been derived in total to specify the various uses cases with the objective to collect user requirements. These are:

- Cybersecurity Professionals
- Telecommunication Operators
- Telecommunication Infrastructure Providers
- Investment Management Positions
- Individual Telecommunication Users

A detailed description of the planned activities as well as considerations regarding the collection and processing of personal data associated with the user requirements elicitation process can be found in the Deliverable D9.8 (“POPD-Requirement No. 8”).

The analysis includes considerations for the measures that should be adopted, if applicable, like anonymization techniques in the submitted online questionnaire, to allow for the adoption of the approach presented in the Deliverable D9.1 (“H-Requirement No. 1”). In D9.1, it is indicated in more details that the participants involved in the requirement elicitation process can be selected within the staff of SPIDER partners, or closely related network of experts, without the need of informed consent, as appropriate and applicable each time, as no personal data will be collected to the least extent possib**le.** Indeed, the questionnaires to be distributed to the research participants will be completely anonymous and will not require any personal data from the participant. The participants will not be asked to login nor to submit their email addresses (or any other personal information) in order to take

part in the survey. Only the participants' answers to multiple-choice questions will be collected. No personal data will be collected.

Yet, in fulfilment of the relevant ethics requirements, the information sheet and the consent form templates are annexed to the Deliverable D9.1 ("H-Requirement No. 1). For more details about the informed consent procedures please refer to D9.1.

4.2 Privacy Protection Issues in Pilot Use Case Scenarios

The WP7 activities that have been taken into consideration for the analysis of potential personal data protection aspects are divided into the following pilot use cases:

- PUC1.a: Cybersecurity Testing of 5G-ready applications and network services (Task 7.2)
- PUC1.b: Cybersecurity of Next Generation Mobile Core SBA (Task 7.3)
- PUC2.a: 5G Security Training for Experts (Task 7.4)
- PUC2.b: 5G Security Training for Non-Experts (Task 7.4)
- PUC3: Cybersecurity Investment Decision Support (Task 7.5)

In the context of the Deliverable D9.8 ("POPD-Requirement No. 8), all five pilot testing activities have been taken into consideration for the analysis of potential ethics concerns relative to the collection and processing of personal data. A preliminary analysis of the privacy protection issues in the SPIDER pilot use case scenarios, as conducted by the pilot partners at the time of writing this deliverable, is presented in Table 1. The provided ethics summary also contains information from the ethics perspective of humans' participation in the SPIDER pilot use cases.

Table 1 Ethics summary of the SPIDER pilot use case scenarios

Pilot Use Case	Ethics Summary
PUC1a	• **NO human participants** will be involved. • **NO personal data** will be collected. • **NO** real end telecommunication systems operating end-user's communications will be involved. • **NO real user traffic** will be collected. Only **simulated/synthetic traffic** will be used or, for the traffic generated by the trainees during their participation, it will not be possible to link to the participants.
PUC1b	• **NO human participants** will be involved. • **NO personal data** will be collected. • **NO real user traffic** will be collected. Only **simulated/synthetic traffic** will be used or, for the traffic generated by the trainees during their participation, it will not be possible to link to the participants.
PUC2a PUC2b	• There will be **human participants**, but • **NO personal data** will be collected.
PUC3	• **NO human participants** will be involved. • **NO personal data** will be collected.

It is evident from Table 1 that in all five pilot use case scenarios of the SPIDER project:

(a) **no personal data** will be collected;
(b) **no real user traffic** will be collected (only simulated/synthetic traffic will be used).

Since **no personal data will be collected**, this fact minimises the risks associated with the collection, storage and processing of data without decreasing the accuracy of the studies.

As a result of the detailed analysis provided in the Deliverable D9.8 ("POPD-Requirement No. 8) regarding the various use cases for demonstration and evaluation testing as part of the tasks in WP7, some highlights can be derived:

- The strict compliance with the relevant EU legal framework [2] and guidelines ([20], [21]) will be maintained throughout the project lifecycle. This approach will minimize any possible risk.
- Since no personal data will be collected during pilots, we **do not foresee any particular risks related to data processing**.
- UK-based partners will continue to be compliant with EU Regulations also after the Brexit.
- Data breach risks will be reduced by adopting appropriate security measures.

Overall, from the analysis conducted in the Deliverable D9.8 ("POPD-Requirement No. 8"), it has been concluded that the SPIDER research activities conducted under the Work Packages WP2 and WP7 **do not present an ethics risk to research participants from a privacy and data protection point of view**.

In fulfilment of the relevant ethics requirements, the information sheet and the consent form templates are annexed to the Deliverable D9.1 ("H-Requirement No. 1")

5 LEGAL AND ETHICAL FRAMEWORK FOR THE INVOLVEMENT OF HUMAN SUBJECTS IN THE PILOT TESTING

The overall objective of the SPIDER project is to develop, pilot test and disseminate a Cyber Range as a Service (CRaaS) platform whose goal is to provide virtualised 5G cyber range services to 5G telecommunications providers, cyber security professionals, ICT vendors, etc. Within the remit of the SPIDER project, one main ethical question arises:

- Will participants involved in the pilot testing be exposed to any harm?

According to Frankel and Siang [6], "*the current ethical and legal framework for protecting human subjects, rests on the principles of autonomy, beneficence, and justice*". Autonomy is assured via the process of informed consent[1], in which the risks and benefits of the research are disclosed to the subject. Beneficence maximizes the benefits of the research while minimizing the risks to the subjects. The principle of justice requires a fair distribution of the risks and benefits associated with the research.

Similar to Frankel and Siang, the Ethical Impact Assessment (EIA) of Kenneally *et al.* [7], and the Belmont report [8] base their framework on the three ethical principles of autonomy, beneficence and justice. However, instead of autonomy they use the term "respect for persons" to incorporate the two ethical convictions: to treat subjects as autonomous agents and secondly to take care to protect persons with diminished autonomy.

The IEA and Akiyama & Yoshioka [9] extend the definition of "Respect for Persons" by treating organisations in as similar fashion as human subjects. Akiyama and Yoshioka show how they limit the harm inflicted to the organisations they research by anonymising the involved parties and responsibly disclosing security vulnerabilities.

The Menlo report [10] extends the "Respect for Persons" principle by including the non-research subjects that are directly interfaced, integrated with, or impacted by the study of the computer systems and data. The report also introduces a fourth principle called "Respect for Law and Public Interest". This principle is an implicit part of the beneficence principle. It requires the research to be compliant, transparent and accountable. Compliance requires researchers to identify laws, regulations, contracts and private agreements applicable to the research. Transparency refers to the transparent methodologies and results. Accountability requires methodologies, ethical evaluations, collected data and results to be documented and disclosed responsibly.

[1] Article 4 (11) of the GDPR defines consent of the data subject as "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*".

6 HUMAN PARTICIPANTS IN RESEARCH ACTIVITIES AND POTENTIAL ETHICAL CONCERNS

This section focuses on ethical considerations that will guide human participation in the SPIDER requirements collection, use cases and validation pilot testing, with particular reference to obtaining the voluntary and informed consent. According to Deliverable D9.1 ("H - Requirement No. 1") the activities that require consideration of ethical aspects concerning the involvement of human participants in the SPIDER project relate to the following categories:

1) participation in the requirements-gathering activities of WP2,
2) participation in the project pilot activities of WP7,
3) participation in workshops or other similar communication or disseminations activities.

6.1 REQUIREMENTS-GATHERING ACTIVITIES OF WP2

6.1.1 Recruitment process

As mentioned before, the WP2 activities that potentially foresee human participation and informed consent procedures are those related to T2.1 "Analysis of User and Cybersecurity Requirements". This task has the primary goal to specify the different types of users of the SPIDER platform, considering both cyber security experts as well as non-experts, using different real users' profiles with a variety of expertise and multiple professional orientations.

Based on the stakeholder categories identified in T2.1 and presented in section 4.1, it has been concluded that either members of the SPIDER partners or members of the network of the SPIDER partners with legal relationships already established will be used as participants in the requirement elicitation process. Accordingly, there will be no open call for participation**.** The SPIDER partners involved in the requirements collection have an extended knowledge base within the colleagues with proper experience that will provide the required support for WP2. There are benefits with this approach:

- the stakeholders involved can be selected being both relevant and appropriate to the project;
- the participants will be more easily accessible by the SPIDER partners and the managerial issues (i.e., training, meetings and briefing) can be handled in a structured, organised and efficient way); and
- the participants can be selected in order not to be biased or related to SPIDER in any way.

Details about the planned activities for the requirements collection along with indications of how the involvement of the participants in the research activities of WP2 is organized can be found in the Deliverable D9.1 ("H - Requirement No. 1"). The presented analysis highlighted that **no evidence of an ethics risk exists for the research participants** given that they will be asked to fill in an **anonymous online questionnaire**, where **no personal data will be collected**. However, in fulfilment of relevant ethics requirements, the information sheet and the consent form templates are annexed to the Deliverable D9.1 ("H-Requirement No.1).

6.1.2 Informed consent procedure

As analysed before, the human participation in the requirements collection activities of the WP2 does not involve the collection and/or processing of personal data. Despite this fact, the SPIDER partners are fully aware of the need to respect fundamental principles of ethics that serve to protect the interests of the research participants. Accordingly, and as further detailed in D9.1 ("H – Requirements No. 1"), the SPIDER consortium will seek only the freely given, specific, informed and unambiguous consent expressed in clear and plain language. Moreover, the volunteer participant will always have the opportunity to freely withdraw, without consequences.

The informed consent form and information sheet regarding the involvement of humans in the SPIDER's requirements collection activities are enclosed in the Deliverable D9.1 ("H - Requirement No. 1"). Please refer to D9.1 for more information about the informed consent procedures that will be implemented for the participation of humans in the WP2 activities of the SPIDER project.

6.2 PROJECT PILOT ACTIVITIES OF WP7

6.2.1 Recruitment processes for pilot testing

As detailed in Chapter 4.2, the WP7 activities that have been taken into consideration for the analysis of potential human participation are related to:

- T7.2 "Cybersecurity Testing of 5G-Ready Applications and Network Services Pilot",
- T7.3 "Cybersecurity of Mobile Core SBA Pilot",
- T7.4 "5G Security Training Pilot", and
- T7.5 "Cybersecurity Investment Decision Support Pilot".

For the project pilot activities of WP7, Deliverable D9.1 ("H - Requirement No. 1") contains a detailed description of the planned activities with an indication of how the involvement of participants into the pilot activities of the SPIDER project is organized. From the analysis, the design of the pilot use cases has driven to the conclusion that **all the participants in the project pilots will be members of the network of the SPIDER partners**. The human participants comprises a mix of staff already working in the project, colleagues with proper experience currently employed by the SPIDER partners, or experts with already established relationship with SPIDER partners. Accordingly, there will not be an open call for participation.

The approach to involve participants in the pilots from a well and extensive network of contacts, like the one applied for WP2, gives the same benefits plus the following:

- Given that part of the evaluation will be based on the pilot participants, these need to be selected to make sure that the proper non-biased experts will be the one to evaluate various parameters of the solution.
- These participants can support post-test analysis or even repeated pilot runs (if needed).

6.2.2 Informed consent procedure

From the analysis conducted in Deliverable D9.1 ("H - Requirement No. 1"), it has been concluded that **there is no evidence of ethics risks for the research participants** taking part in the SPIDER pilot activities as part of WP7. In fulfilment of the relevant ethics requirements, the information sheet and the consent form templates are annexed to the Deliverable D9.1 ("H-Requirement No.1).

6.3 WORKSHOPS & DISSEMINATION

In addition to the research activities identified as part of WP2 and WP7, proper ethical consideration is also required for the human participants in the SPIDER workshops and other similar communication or dissemination activities.

Apparently, the participant's basic contact information is required for allowing an efficient organisation and management of events, such as workshops. This enables the project's contact list management, event invitations, reports circulation and feedback management, follow ups and meetings, etc.

Among the personal data usually required during the registration process there are title, first name and family name, organisation name, email address, postal address, organisation address, profession/position, and phone/fax number.

An identity document (passport/identity card) may also be required to prepare the entrance permissions and access control by the security guards to the premises where the event takes place. In this case, the legal basis for processing of data is public interest (security). More personal data may refer to individual requirements, e.g., diet or mobility (this only to ensure that they are taken into account but not used or stored beyond the single event).

In case any of the workshops or similar events are organised in collaboration with an external service provider (e.g. EDAS), this entity will share the responsibility for legal compliance during the event. The responsibilities of the service provider as well as its status (data controller / data processor) in terms of GDPR compliance will be regulated by a contract.

For online seminars and demonstrations that will be organized by the SPIDER partners, the selection and recruitment procedures adopted will be organized in such a way that they do not foresee the collection of any personal data.

In consideration of the procedure and the assumptions outlined above, the informed consent procedure for the human participation, which has been investigated for potential adoption into the SPIDER research activities, **is not applicable to the workshops, and to similar dissemination and communication activities** when the partner organization relies on a specialised service company for what concerns the arrangements and recruitments.

7 ETHICAL, PRIVACY AND LEGAL REQUIREMENTS

7.1 REQUIREMENTS DEFINITION

In this section, we summarise the ethical, privacy and legal requirements of the SPIDER platform along with the Key Performance Indicators (KPIs) that will be used to assess the ethical, privacy and legal aspects of the SPIDER platform during the pilot testing phase. For the analysis, we used input from the ethical, privacy and legal review conducted in the previous sections of this document. The template used for the identification of the requirements shown in Table 2 has been organised as follows:

- **Requirement ID** (in the form EPLR-ID)
- **Title**
- **Description**
- **Category** (ethical, legal, privacy)
- **Source**
- **Relevant Ethics Deliverable**
- **Relevant KPI**
- **Way to measure the KPI**

Table 2 SPIDER ethical, privacy and legal requirements

Requirement ID	**EPLR-001**
Title	Personal data processing consent
Description	Personal data shall not be processed without a legal ground or the agreement of the data subject. The data subject has to give his/her consent to the processing of his or her personal data for one or more specific purposes which should documented by the data controller.
Category	Privacy, Legal
Source	GDPR
Ethics Deliverable	D9.1 (“H - Requirement No. 1”)
Relevant KPI	Percentage of data subjects that provided consent = 100%
Way to measure the KPI	Match the participants to the collected consent forms

Requirement ID	**EPLR-002**
Title	Data subjects’ rights
Description	Clear procedures shall be in place to ensure data subjects’ rights, by all data controllers, namely: 1. Right of access to their data and to receive any important information on what it is done with the data; 2. Right to rectification, when the personal data are processed in a non-accurate way; 3. Right to erasure, under certain conditions, in particular when data have been processed unlawfully or are no longer necessary; 4. Right to restriction, meaning the right to “freeze” data and obtain that they are not processed for a certain period of time, for

	example when the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data); 5. Right to data portability; 6. Right to object.
Category	Privacy, Ethical
Source	GDPR
Ethics Deliverable	D9.7 ("POPD - Requirement No. 7")
Relevant KPI	Number of data subjects' rights procedures in place for each data controller = 6
Way to measure the KPI	Data controller(s) provide documentation/proof of procedures in place.

Requirement ID	**EPLR-003**
Title	Data breach notification procedures
Description	A standardised procedure to handle and notify Data Breaches to Data Protection Authorities and Data Subjects concerned must be in place.
Category	Privacy, Legal
Source	GDPR
Ethics Deliverable	D9.7 ("POPD - Requirement No. 7")
Relevant KPI	Percentage of data breaches notified to the authorities and the data subjects = 100%
Way to measure the KPI	Evidence of communication with the authorities and the data subjects for each data breach event.

Requirement ID	**EPLR-004**
Title	Security and confidentiality of network communications
Description	Electronic Communication Services and Networks must be secured through appropriate technical and organizational measures (e.g., encryption). Moreover, the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, must be ensured.
Category	Privacy
Source	ePrivacy Directive
Ethics Deliverable	D9.7 ("POPD - Requirement No. 7")
Relevant KPI	Percentage of unencrypted traffic communicated via a public communications network = 0%
Way to measure the KPI	Technical documentation of all communication channels showing that encryption algorithms are in place.

Requirement ID	EPLR-005
Title	Data anonymization
Description	Violations of privacy and data protection shall be prevented by deploying anonymization techniques (e.g., attribute suppression, character masking, etc.) in all data collected and processed.
Category	Privacy, Ethical
Source	-
Ethics Deliverable	D9.1 (“H - Requirement No. 1”) D9.3 (“POPD - Requirement No. 3”) D9.7 (“POPD - Requirement No. 7”)
Relevant KPI	Percentage of anonymized data sets = 100%
Way to measure the KPI	Data sets collected during pilots to be made available to third parties to ensure that no personal identifiable information (PII) is present.

Requirement ID	EPLR-006
Title	Personal data collection during pilot use cases
Description	No personal data shall be collected during SPIDER pilot use case scenarios.
Category	Ethical, Privacy
Source	-
Ethics Deliverable	D9.7 (“POPD - Requirement No. 7”) D9.8 (“POPD - Requirement No. 8”)
Relevant KPI	Amount of personal data records collected during the pilot use case = 0
Way to measure the KPI	Data sets collected during pilots to be made available to third parties to ensure that no personal identifiable information is present.

Requirement ID	EPLR-007
Title	Usage of telecommunication systems during pilot use cases
Description	No real telecommunication systems operating end-user’s communications will be involved during SPIDER pilot use case scenarios.
Category	Ethical, Privacy
Source	-
Ethics Deliverable	D9.7 (“POPD - Requirement No. 7”) D9.8 (“POPD - Requirement No. 8”)
Relevant KPI	Real telecommunications systems involved in the pilot use case = 0
Way to measure the KPI	Information about the telecommunications system used in each pilot to be made available (i.e., testbed, network digital twin, or real production)

Requirement ID	EPLR-008
Title	Usage of user traffic data during pilot use cases
Description	No real user traffic shall be collected during the SPIDER pilot use case scenarios. Only simulated/synthetic traffic will be used or, for the traffic

Requirement ID	EPLR-008
	generated by the trainees during their participation, it will not be possible to link to the participants.
Category	Ethical, Privacy
Source	-
Ethics Deliverable	D9.7 (“POPD - Requirement No. 7”) D9.8 (“POPD - Requirement No. 8”)
Relevant KPI	Amount of traffic user data collected in the pilot use case = 0
Way to measure the KPI	Percentage of user traffic data that is synthetic or originates from public sources (excluding data generated from trainers) = 100% No personal identifiable information (PII) is present in the data generated by the trainees.

Requirement ID	EPLR-009
Title	Cookie law
Description	The SPIDER website(s) should provide clear information on the cookies it will potentially deploy into the users’ devices and require users to opt-in. So, the SPIDER websites must block cookies, until visitors have given their informed consent to their use.
Category	Privacy, Legal
Source	EU Cookie Directive
Ethics Deliverable	-
Relevant KPI	Percentage of the SPIDER website(s) obtaining user consent before deploying cookies = 100%
Way to measure KPI	Website admin(s) to provide evidence of cookie-related procedures deployed in the SPIDER website(s) related to the project.

Requirement ID	EPLR-010
Title	Location data principles
Description	Any user location data collected by the SPIDER website(s) shall adhere to the following principles: 1. Location data can be processed for the provision of value-added services only anonymously or upon specific consent of the user concerned (Consent for Location Data); 2. Users must be given the opportunity to easily refuse such processing at each connection (Updated Consent); 3. Location data must be processed only by persons under the authority of the service provider that are dedicated to the function or unit for which such data are necessary (Authorization profiles).
Category	Privacy, Legal
Source	ePrivacy Directive
Ethics Deliverable	-

Relevant KPI	Number of collected location data principles in place for each SPIDER website = 3
Way to measure the KPI	Website admin(s) to provide evidence of location data handling procedures deployed in the SPIDER website(s) related to the project.

Requirement ID	**EPLR-011**
Title	Traffic data principles
Description	Any user traffic data collected by the SPIDER website(s) shall adhere to the following principles: 1. Traffic data must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication or for the purposes of processing subscriber's billing and interconnection payments (traffic data erasure); 2. Traffic data can be processed for marketing and/or for the provision of value-added services only upon specific consent of the user concerned (Consent for Marketing purposes); 3. Specific information on traffic data processing and its duration must be provided (specific Information); 4. Traffic data must be processed only by persons under the authority of the service provider that are dedicated to the function or unit for which such data are necessary (e.g., handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value-added service – Authorization profiles.
Category	Privacy, Legal
Source	ePrivacy Directive
Ethics Deliverable	-
Relevant KPI	Number of collected traffic data principles in place for each SPIDER website = 4
Way to measure the KPI	Website admin(s) to provide evidence of traffic data handling procedures deployed in the SPIDER website(s) related to the project.

7.2 Mapping Requirements to SPIDER Pilot Use Cases

Table 3 summarises the mapping between the ethical, legal and privacy requirements identified in the previous subsection, and the pilot use case scenarios defined in the Deliverable D2.8 “SPIDER use cases and pilots definition – final version”, which is submitted as part of the Task 2.4 “Design of the SPIDER Pilot Use Cases”, namely:

- PUC1.a: Cybersecurity Testing of 5G-ready applications and network services
- PUC1.b: Cybersecurity of Next Generation Mobile Core SBA
- PUC2.a: 5G Security Training for Experts
- PUC2.b: 5G Security Training for Non-Experts
- PUC3: Cybersecurity Investment Decision Support

Note that the requirements entitled EPRL-009, EPRL-010, and EPRL-011, because they are generic by referring to the SPIDER website(s), they do not apply to the SPIDER pilot use cases and as such they are not mapped in Table 3.

Table 3 Mapping the ethical, privacy and legal requirements to SPIDER Pilot Use Cases

Requirement ID	SPIDER Pilot Use Case Scenarios				
	PUC1.a	PUC1.b	PUC2.a	PUC2.b	PUC3
EPRL-001			+	+	
EPRL-002			+	+	
EPRL-003			+	+	
EPRL-004	+	+	+	+	+
EPRL-005	+	+	+	+	+
EPRL-006			+	+	
EPRL-007	+	+	+	+	+
EPRL-008	+	+	+	+	+

As it can be seen from Table 3, the 5G Security Training pilots (PUC2.a and PUC2.b) necessitate close monitoring of their ethical and privacy-related aspects due to the fact that both pilots consider the involvement of human subjects in their trials. This is not the case for the remaining three pilot use cases (PUC1.a, PUC1.b, and PUC3) since no human participants is envisaged in all of them (see Section 4.2 for details). Another finding is that four requirements, namely the EPRL-004, EPRL-005, EPRL-007 and EPRL-008, are applicable to all five SPIDER pilot use cases. These four requirements relate to the SPIDER platform itself and its 5G emulated environment, which is detailed in D2.7 “SPIDER platform reference architecture – final version”, and as such, they should be monitored throughout the pilot testing phase of all five SPIDER pilot use cases.

8 CONCLUSIONS

Deliverable D2.6 “SPIDER Ethical, Privacy and Legal Requirements – final version” has detailed European and national frameworks for handling ethical, legal and data protection issues in Horizon 2020 research and innovation projects, like SPIDER. This deliverable aimed to identify key issues that can arise throughout the lifecycle of the SPIDER project, considering also aspects specific in each pilot country (Italy, Spain, Greece and UK).

This deliverable first investigated the corresponding European directives including the General Regulation for Data Protection (GDPR), the e-Privacy Directive and Cookie Directive with the support of all national frameworks of the pilot countries (Italy, Spain, Greece and UK). An ethical summary of the SPIDER pilot scenarios has been presented and solutions on how to address them have been provided, considering the involvement of human subjects. Ethical principles were also summarised for the use of all partners and other Work Packages. Finally, KPIs were associated to the elicited ethical, privacy and legal requirements of the SPIDER platform allowing for the assessment of the ethical, privacy and legal aspects of the platform during the pilot testing phase.

The research conducted in this deliverable includes several important aspects of privacy and data protection from both an EU and national regulatory framework and technical perspective. The ethical analysis will be of interest to all work packages of the SPIDER project. The presented guidelines will be a reference for technical and pilot partners of the SPIDER platform both during the implementation and execution phase, and also for the exploitation of the platform, which the consortium expect the deliverable to reach a wider audience of policy makers and researchers for further projects.

Undoubtedly, the recommendations and good practices presented in this deliverable will ensure full compliance of the SPIDER project to the ethical standards and guidelines of the Horizon 2020 work programme. The outcomes of this deliverable also highlighted that the consortium is in position to introduce effective measures towards the prevention of ethical concerns that might occur during SPIDER’s research and pilot activities.

9 REFERENCES

[1] Grant Agreement Number 833685 — H2020 SPIDER Project

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e40-1-1

[3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

[4] Charter of Fundamental Rights of the European Union (2000/C 364/01), Available online: http://www.europarl.europa.eu/charter/pdf/text_en.pdf

[5] Windley, P. J. (2005). Digital Identity: Unmasking identity management architecture (IMA). " O'Reilly Media, Inc.".

[6] Frankel, Mark & Siang, Sanyin (1999). Ethical and Legal Aspects of Human Subjects Research on the Internet.

[7] Kenneally, Erin & Bailey, Michael & Maughan, Douglas. (2010). A Framework for Understanding and Applying Ethical Principles in Network and Security Research. 240-246.

[8] The Belmont Report. (2014). Ethical principles and guidelines for the protection of human subjects of research. The Journal of the American College of Dentists, 81(3), 4.

[9] Akiyama Mitsuaki & Yoshioka Katsunari. (2018). Cybersecurity Research Ethics and Related Activity in Japan. Business Trends. pp. 1-4.

[10] Dittrich, D., & Kenneally, E. (2012). The Menlo Report: Ethical principles guiding information and communication technology research. US Department of Homeland Security

[11] Spain, Data Protection Laws and Regulations, https://iclg.com/practice-areas/data-protection-laws-and-regulations/spain/

[12] Spanish Data Protection Act ("SDPA"), December 7 2018, https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/spain/

[13] Greek Data Protection Law, August 27 2018, https://iapp.org/news/a/greece-incorporated-gdpr-data-protection-regulation-into-law/

[14] The Greek Bill Law, February 20 2018, https://www.dlapiperdataprotection.com/?t=law&c=GR/

[15] Data Protection Code, Legislative Decree no. 196/2003, August 10 2018, https://www.garanteprivacy.it/web/guest/home_en/italian-legislation

[16] Data Protection Act 2018, 23rd May 2018, http://www.legislation.gov.uk/ukpga/2018/12

[17] SPIDER Deliverable D9.1 (“H – Requirements No. 1”)

[18] SPIDER Deliverable D9.8 (“POPD – Requirement No. 8”)

[19] Opinion 04/2014 on Anonymisation Techniques - Article 29 Data Protection Working Party - 0829/14/EN WP216. Online: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf/

[20] Guidelines on the use of cloud computing services by the European institutions and bodies https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_en.pdf

[21] Ethics and data protection https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf