D2.3 Preliminary ethics and legal framework

Work Package:	WP2
Lead partner:	Sheffield Hallam University (CENTRIC)
Author(s):	Helen Gibson (CENTRIC), Katie Bailey (CENTRIC); with contributions from KEMEA, NOA, HP, DEIMOS, DEM, FMI, SERCO, ENG, CERTH.
Due date:	30/04/2021
Version number:	1.0 **Status:** Final
Dissemination level:	Public

Project Number:	883284 **Project Acronym:** 7SHIELD
Project Title:	Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats
Start date:	September 1st, 2020
Duration:	24 months
Call identifier:	H2020-SU-INFRA-2019
Topic:	SU-INFRA01-2018-2019-2020 Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe
Instrument:	IA

Horizon 2020
European Union Funding
for Research & Innovation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883284

Revision History

Revision	Date	Who	Description
0.1	28/03/2021	CENTRIC	Table of Contents
0.2	5/04/2021	CENTRIC	1st Draft
0.3	16/04/2021	CENTRIC	Incorporation of partner inputs (KEMEA, HP, SERCO, FMI, NOA, DEIMOS, DEM, SPACEAPPS, ENG)
0.4	19/04/2021	CENTRIC	Version for review
0.5	25/04/2021	CENTRIC, DFSL, ACCELI	Updates to address DFSL and ACCELI peer review comments & addition of exec summary. Finalisation of deliverable
1.0	30/04/2021	ENG, CERTH	Final review and version ready for submission

Quality Control

Role	Date	Who	Approved/Comment
Internal review	23/04/2021	DFSL	Approved with minor comments / suggestions
Internal review	22/04/2021	ACCELI	Approved with minor comments / suggestions

Disclaimer

This document has been produced in the context of the 7SHIELD Project. The 7SHIELD project is part of the European Community's Horizon 2020 Program for research and development and is as such funded by the European Commission. All 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 user thereof uses the information at its sole risk and liability. For the avoidance of all doubts, the European Commission has no liability with respect to this document, which is merely representing the authors' view.

Executive Summary

The security and resilience of ground segments of space systems against physical and cyber threats is essential for ensuring the safety of European citizens. Through the provision of data and services relating to earth observation, satellite communication and navigation, the data relayed through the operation of ground segments are both a critical infrastructure and a provider of information to protect and monitor other European critical infrastructures. 7SHIELD aims to develop a system which better protects, European ground segments against cyber and physical attacks through the development of prevention, detection, response, and mitigation technologies.

The protection of critical infrastructure, the management of personal data, the development of 7SHIELD technologies and the associated research activities all operate with the legal framework of the European Union whilst technologies must be developed in an ethical and socially conscious manner. This deliverable sets forth the initial scoping framework in which 7SHIELD will operate.

7SHIELD as a research project and as an operational system must both respect and help to protect the fundamental rights of the citizens of Europe and ensure that their data is appropriate managed through all activities and interactions with the project and the system. The General Data Protection Regulation (GDPR) has been a transformational piece of legislation for the protection of personal data within Europe. Understanding, documenting and mitigating against the risks of processing personal data is essential for 7SHIELD. The principles of data protection, methods of establishing the lawfulness of processing, and the impact of processing special categories of personal data, the conditions for consent and the effect of advanced technologies such as artificial intelligence are all considered within the scope.

Furthermore, the evolving legislation surrounding the resilience of critical entities and the update to the directive concerning network and information systems security will have a significant impact on how European Union Member States manage the resilience of critical infrastructure over the next decade. For 7SHIELD to be at the heart of such development, a clear understanding of the current and the future legal environment is essential.

Technological innovations such as artificial intelligence, the deployment of drones, video surveillance and facial recognition, use of wearable sensors and the application of social media, amongst others, all have the power to have a significant impact on the efficiency and effectiveness of monitoring large physical and cyber infrastructures. However, such technologies must also operate in the appropriate legal environment: from complying with data protection principles to flying safely.

As well as European level legislation, each Member State has a national implementation of EU law, whilst also developing their own national legislations. In 7SHIELD, it is important to ensure that the pilot countries (Belgium, Finland, Greece, Italy and Spain) clearly

understand the legal context of their own country and any specific requirements for 7SHIELD. This is covered in an initial version in this deliverable and will be covered in more depth in the second iteration of the deliverable.

Ethical and societally responsible application of technologies is imperative for establishing trust with European citizens, employees of the organisations utilising the systems and to ensure they accurately achieve their aims. 7SHIELD must employ ethical practices in the application of artificial intelligence through limiting and mitigating the potential for bias, ensuring that the understanding of the effects of the disruption to critical infrastructure do not have disproportionate cascading effects on certain groups, methods for ensure appropriate vulnerabilities disclosure and how the use of different communication media may limit of extend the reach of various messages.

Finally, 7SHIELD is first and foremost a research project, and while the majority of data protection and ethics requirements are covered in WP9 it is also important to ensure that national legislations that are applicable to research in Member States is accurately applied, especially in respect Article 9(2)(j) of the GDPR.

Overall, this deliverable ensures that the foundation for understanding and situating all aspects of the 7SHIELD project within the legal and ethical environment in which it sits are considered. This will feed forwards into the user requirements, security requirements, planning of piloting activities, and eventually the potential for operational implementation. The next iteration of the framework will build on this foundation to give a deeper treatment of all technological components and piloting activities.

Table of Contents

Executive Summary 4
1. Introduction 11
1.1. Overview 11
1.2. Context and scope 11
1.3. Deliverable structure 13
2. General legal framework 15
2.1. Fundamental rights 15
2.2. General data protection regulation 16
2.2.1. Core principles of data protection 19
2.3. Relevant legislation for 7SHIELD domain 23
2.3.1. Protection of national critical infrastructure 23
2.3.2. Space ground segments 25
2.3.3. Cybersecurity 27
3. Legal considerations for 7SHIELD technology 30
3.1. Prevention technologies 30
3.1.1. Risk and vulnerability assessments 31
3.1.2. Secure authentication 32
3.1.3. Cascading effects (& prevention of) 33
3.2. Detection technologies 33
3.2.1. Online data acquisition 34
3.2.2. Video surveillance 36
3.2.3. Processing image and video data 37
3.3. Response technologies 38
3.3.1. Semantic modelling 39
3.3.2. Wearables and health data 39
3.3.3. Social media communications 39
3.3.4. Drone operations 40
3.3.5. Autonomous operation of drones and drone neutralisation 43
3.4. Mitigation technologies 43
4. National legislation for the pilot use case countries 45
4.1. PUC1 Arctic Space Centre, Finland 45
4.2. PUC2 DEIMOS Ground Segment, Spain 46
4.3. PUC3 National Observatory of Athens Ground Segment, Greece 49
4.4. PUC4 ICE Cubes Service 55
4.5. PUC5 ONDA DIAS Platform 56
5. Ethical and societal framework 60
5.1. Ethics and societal impact on the space sector 60
5.2. Societal and ethical considerations for 7SHIELD technologies 60
5.2.1. Prevention technologies 62
5.2.2. Detection technologies 63
5.2.3. Response technologies 66
5.2.4. Mitigation technologies 67
6. Legal and ethical considerations for 7SHIELD research 69
6.1. National data protection laws for pilot countries 69
6.2. Ethical considerations relating to piloting activities 73
7. Conclusions 75

7.1. Summary 75
7.2. Next steps towards the final framework 75
Annex I: End User Questionnaire 76

List of figures

Figure 1: Framework for 7SHIELD demonstrating the proposed technologies and different aspects of the system (retrieved from https://www.7shield.eu/concept/) 30
Figure 2: Overview of rules and regulations for the operation of drones in the open category 42

List of Tables

Table 1 - Pilot Use Cases (PUC) in 7SHIELD 12

Definitions and acronyms

AEPD	Agencia Española de Protección de Datos (Spanish Data Protection Agency)
AI	Artificial Intelligence
API	Application Programming Interface
ASI	Agenzia Spaziale Italiana
BVLOS	Beyond Visual Line of Sight
CCTV	Closed Circuit Television
CI	Critical Infrastructure
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CoE	Council of Europe
CFR	Charter of Fundamental Rights of the European Union
CSIRT	Computer Security Incident Response Team
C/P	Cyber/Physical
DIAS	Data and Information Access Services
DPIA	Data Protection Impact Assessment
DSPs	Digital Service Providers
DPO	Data Protection Officer
EASA	European Union Aviation Safety Agency
EC	European Commission
ECI	European Critical Infrastructure
ECHR	European Charter on Human Rights
ECSL	European Centre for Space Law
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EGNOS	European Geostationary Navigation Overlay Service
ENISA	European Union Agency for Cybersecurity
ENAC	Ente Nazionale per l'Aviazione Civile (Italian Civil Aviation Authority)
EO	Earth Observation
EPCIP	European Programme for Critical Infrastructure Protection
ERNCIP	European Reference Network for Critical Infrastructure Protection
ESA	European Space Agency
EU	European Union
GDPR	General Data Protection Legislation
GNSS	Global Navigation Satellite System
GS	Ground Segment
GSA	Global Navigation Satellite Systems Agency
HCAA	Hellenic Civil Aviation Authority
HLEG	High Level Expert Group
HP	Hellenic Police
IA	Information Assurance
ICO	Information Commissioner's Office
MS	Member States

NAA	National Aviation Authority
NIR	Near Infrared
NIS	Networks and Information Systems
NOTAM	Notice to Airmen
OES	Operators of Essential Services
OSPs	Operator Security Plans
PD	Presidential Decree (Greece)
PUC	Pilot Use Case
REP	Robots Exclusion Protocol
SATCOM	Satellite Communications
SLOs	Security Liaison Officers
UAVs	Unmanned Aerial Vehicles
VLOS	Visual Line of Sight
WP	Work Package

1. Introduction

1.1. Overview

7SHIELD (Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response, and mitigation of physical and cyber threats) is aimed at addressing the security and resilience of Ground Segments (GS) of Space Systems. Such systems provide enormous amounts of critical satellite data for earth observation (EO), satellite communications (SATCOM) and global navigation satellite systems (GNSS). European citizens, public sector and commercial sector services all depend on access to these services every day.

The safety and security of GS are essential as a critical infrastructure (CI) themselves but the data they provide are also used for monitoring other CI sites and for supporting emergency response in the event of a major disaster. Such sites must have adequate protection and resilience to prevent and respond to both natural disasters and man-made attacks that impact the physical environment and cyber operations within the ground segment. A recent article has considered some of the most prevalent upcoming threats to the space sector[1].

To protect such infrastructure, 7SHIELD foresees the development of a comprehensive system that provides a range of technological components and a series of pilot demonstration events that envisage how the system would be deployed and used operationally. An important consideration is the legal and ethical framework in which the deployment of such advanced technologies would exist.

This deliverable has been prepared in the context of *T2.4 – Ethics and Legal Framework* as part of 7SHIELD WP2 (User Requirements and Use Cases Design). This deliverable follows *D2.1 – 7SHIELD Use Cases Design* and *D2.2 – Consolidation of Stakeholder Requirements*. This deliverable will be the first version of the legal and ethical framework and will be followed by a consolidation of all legal and ethical considerations for the 7SHIELD project and system in Month 22 of the project (June 2022).

1.2. Context and scope

As mentioned in the section above, this deliverable appears following the first round of deliverables relating to the 7SHIELD Use Case Design and the Consolidation of Stakeholder Requirements. Due to the classified status of those two deliverables, in D2.3 we make only high-level reference to their contents and instead focus the framework around addressing the key legal and ethical considerations relating to the project that are already in the public

[1] Manulis, M., Bridges, C. P., Harrison, R., Sekar, V., & Davis, A. (2020). Cyber security in New Space: Analysis of threats, key enabling technologies and challenges. International Journal of Information Security, 1-25. https://link.springer.com/article/10.1007/s10207-020-00503-w

domain (such as from the 7SHIELD website[2], the EC CORDIS[3] service and other public 7SHIELD deliverables and contain make no reference to EU Classified Information (EUCI) or confidential project information). In particular, we consider the core innovations under the banner of prevention, detection, response and mitigation technologies; how they are addressed in European and national legal frameworks and any relevant ethical issues. The national legal frameworks considered are those from each of the 7SHIELD pilot countries (as shown in Table 1 below).

Table 1 - Pilot Use Cases (PUC) in 7SHIELD

PUC ID	PUC title	Location
PUC1	Physical Attack in Arctic Space Centre in Sodankylä	Finland
PUC2	Cyber-physical attack in Deimos Ground Segment	Spain
PUC3	Cyber-physical attack in the Ground Segment of NOA in Athens	Greece
PUC4	Threat detection and mitigation on the ICE Cubes Service	Belgium
PUC5	Cyber-attack on the ONDA DIAS platform	Italy

In the vision for 7SHIELD there are several key touchpoints where legal and ethical requirements play an important role. The first of these is the context for the whole project. This context covers the fundamental motivation for the project itself in the work programme[4] – the protection of European Critical Infrastructure (ECI) to ensure that the liberties of European citizens and the functioning of society and our economies are not put at risk. The 7SHIELD deliverable D8.4 Market Analysis Report[5] provides an excellent overview of where GS fit into the Space Sector noting there are three main functions – EO, SATCOM and GNSS.

In respect of EO, it is not only that a GS can be considered a CI itself, EO also plays a vital role in the protection of other CIs and can be used for monitoring hard to reach areas in the event of a disaster, supporting search and rescue operations as well as a plethora of other monitoring activities.[6] EO also has a significantly increasing commercial role with demand for access continuing to soar.[5]

Similarly, SATCOM is used for all kinds of communication activities including television, telephone, radio, and internet supporting civil and military applications. The European

[2] https://www.7shield.eu/
[3] https://cordis.europa.eu/project/id/883284
[4] European Commission (2020) Horizon 2020 Work Programme 2018-202. 14 – Secure Societies – Protecting the freedom and security of Europe and its citizens. (pp. 10-13) https://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-security_en.pdf (last accessed: 21 March 2021)
[5] Pothrat, X. (2021) Market analysis report v1. Deliverable 8.4 of the 7SHIELD project funded under the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement Number 883284.
[6] ESA (2018) The Safety and Security of Critical Infrastructures. European Space Agency, 9 May 2018. https://business.esa.int/news/safety-and-security-critical-infrastructures (last accessed: 21 March 2021)

Commission (EC) has identified several areas where SATCOM can play a significant role in ensuring the safety and security of Europe.[7]

Finally, GNSS are used extensively to transmit positioning and timing data that are used in a variety of sectors including agriculture, aviation, location-based services, mapping and surveying, maritime, rail and road as well as timing and synchronisation activities.[8]

From the above it is clear that GS have an important role to play as critical infrastructure themselves and also as the providers of services to protect other aspects of ECI to ensure the safety and security of European citizens.

At the next level is the protection of the GS against physical attacks and the information stored and accessed through them against cyber-attacks. This includes both the satellite data as well as data about users and employees working with such systems. The technology deployed by 7SHIELD has a duty to uphold the protection of the systems against such attacks and negate the access to such data by unauthorised persons but also must ensure that it is compliant with the legal frameworks and ethical and societal norms expected of such a system and technology.

Across all these aspects, 7SHIELD must also ensure that the research activities undertaken are conducted in a manner which is compliant with European values and expectations of research ethics. Particularly, with respect to the piloting activities and future system operation considerations at each of these sites.

1.3. Deliverable structure

Structure of the remainder of the deliverable

- Chapter 1 explains the overall scope and structure of the deliverable and its position within the 7SHIELD project.
- Chapter 2 covers the general legal framework within which the project sits at a European level. This includes a discussion on fundamental rights, the General Data Protection Regulation, and specific legislation relating to the 7SHIELD domain (critical infrastructure, space ground segments and cybersecurity).
- Chapter 3 reviews any specific legislation relating to the deployment of specific technologies within 7SHIELD across the four layers of the system: prevention, detection, response, and mitigation.
- Chapter 4 expands the legal framework to cover specific aspects relating to the 7SHIELD system through the lens of the pilot countries. This provides a detailed view of the aspects within the general legal framework as they are realised at a

[7] PwC & Ecorys (2016) Satellite Communication to support EU Security Policies and Infrastructures. European Commission https://ec.europa.eu/docsroom/documents/16147/attachments/1/translations/en/renditions/pdf

[8] GSA (2016) GNSS Applications – Segment Pages. European Global Navigation Satellite Systems Agency, 22 March 2016. https://www.gsa.europa.eu/gnss-applications/segment-pages (last accessed: 21 March 2021)

national level (focused on Belgium, Finland, Italy, Greece and Spain as the pilot countries).

- Chapter 5 moves into the ethical and societal framework detailing ethical issues relating to the GS in the space sector; this is followed by the ethical and societal issues relating to any aspects of the 7SHIELD pilots and piloting countries and finally considers the 7SHIELD technologies. Here we also briefly discuss ethics in relation to research and align to the Ethical Requirements as delivered through WP9.
- Chapter 6 addresses any further specific legal and ethical considerations for research activities focusing of aspects of data protection and piloting activities.
- Chapter 7 the concludes the deliverable and sets forth the roadmap to D2.6.

2. General legal framework

The core aim of the 7SHIELD project is to improve the security and resilience of EU Ground Segments (GS) of Space Systems where they are considered a component of critical infrastructure (CI) within Europe. GS facilitate the provision of satellite data to public bodies, government and first responders, commercial entities, non-governmental organisations, research and ordinary citizens. Thus, an attack or disruption to the GS sector has the potential to have significantly negative impacts on the safety and security of European Citizens. 7SHIELD considers physical attacks which may interfere with the distribution of satellite data, cyber-attacks which may affect the integrity and availability of satellite data, and the consequences of a coordinated cyber-physical attack that would amplify the effects of both.

2.1. Fundamental rights

"Fundamental rights are the basic rights and rights and freedoms that belong to everyone in the EU."[9]

Fundamental rights are there to enforce principles such as dignity, fairness, respect, and equality in both how people live and work within Europe.[9] Much of the legislation across Europe is founded on ensuring that the fundamental rights of its citizens are protected. While fundamental rights apply across a wide range of different aspects of life across the EU, in this deliverable we focus specifically on the rights that are most pertinent to the 7SHIELD project and its goal of supporting the safety and security of European citizens.

In Europe, there are two main frameworks that enshrine the protection of these fundamental rights. The European Convention for the Protection of Human Rights and Fundamental Freedoms which is more commonly known as the European Convention on Human Rights (ECHR)[10] and the Charter of Fundamental Rights of the European Union (CFR)[11].

The ECHR originally entered into force in 1953 and is an international convention by the Council of Europe (CoE) and this applies more widely (covering the 47 members of the CoE) than the CFR which applies only to the 27 EU Member States (MS). In the context of the 7SHIELD project, only Israel is not a member of the CoE; however, Israel has Observer Status within the CoE. Both the UK and Switzerland are members of the Council of Europe and thus party to the ECHR although they are not EU MS.

[9] FRA (2020) What are fundamental rights? European Agency for Fundamental Rights. https://fra.europa.eu/en/about-fundamental-rights (last accessed: 21 March 2021)

[10] Council of Europe (1953) Details of Treaty No.005 Convention for the Protection of Human Rights and Fundamental Freedoms. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005

[11] Charter of Fundamental Rights of the European Union (2016) Official Journal C202, 7 June, pp.389-405. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2016:202:TOC

In 7SHIELD, the main focus is on the protection of critical infrastructure, namely ground segments, in the European context. All piloting activities will take place within EU MS, and therefore when considering fundamental rights, it is the CFR that is considered first and foremost. The most relevant articles with the CFR fall under Freedoms include Article 7 – Respect for private and family life and Article 8 – Protection of personal data. Article 52 ensures that the CFR runs parallel to the ECHR.

2.2. General data protection regulation

The General Data Protection Regulation (GDPR) was introduced into EU legislation following the repealing of Directive 95/46/EC in May 2018. The GDPR (Regulation 2016/679)[12] covers the *"protection of national persons with regard to the processing of personal data and on the free movement of such data"*. Given Article 8 of the CFR asserts that the protection of personal data is considered a fundamental right the GDPR then sets out the specific provisions for ensuring that right is protected.

The GDPR applies to the processing of any personal data by an establishment located within the EU and/or the processing of personal data of persons who are in the EU regardless of the location of the establishment (GDPR Article 3 – Territorial Scope). The GDPR applies to all activities of the 7SHIELD project and any future envisioned application of the 7SHIELD system within Europe.

Within the context of 7SHIELD, partners in United Kingdom, Switzerland and Israel are not directly a party to the GDPR. Under the (currently draft) Trade and Cooperation Agreement between the EU and the UK, a version of the GDPR is enacted in UK legislation as the UK GDPR. The UK is not considered a third country with respect to the GDPR until at the latest June 2021 and not before 30 April 2021 when it is hoped that an adequacy decision will be reached. Both Switzerland and Israel already have adequacy decisions from the EU that recognises that a country provides an adequate level of data protection comparable to the GDPR.[13] The EU, as of 19 February 2021 has launched a draft decision on the adequate protection of the protection of personal data by the United Kingdom.[14]

For all EU countries, the GDPR allows for specific provisions by EU MS on the implementation of some aspects of the GDPR (known as opening clauses and derogations) these are discussed in Section 6.1.

[12] 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. Official Journal L119 4 May 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC

[13] European Commission (n.d.) Adequacy decisions. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last accessed: 21 March 2021)

[14] European Commission (2021) Brexit – Draft decision on the adequate protection of personal data by the United Kingdom – General Data Protection Regulation. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/brexit_en (last accessed: 21 March 2021)

Article 4 sets out numerous definitions in scope of the GDPR; below we refer to a number of these definitions to ensure they are considered consistently across the deliverable.

What is personal data?

The core of the GDPR is the protection of *personal data.* The GDPR refers to personal data as the following:

"'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."

That is, personal data must refer to a living person who can be identified by such data. Data which has been completely anonymised is no longer considered personal data and thus can be processed without restriction.

A subsection of personal data, known as *special categories of personal data*, have additional restrictions in relation to processing. These special categories include data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification purposes, health data, and data concerning a person's sex life or sexual orientation (as set out in Article 9).

What is data processing?

It is specifically the act of *processing* personal data that is considered under the GDPR; processing is defined as the following:

"'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

Therefore, fundamentally all aspects of data management fall under the auspice of processing and consequently any action involving personal data falls under the GDPR.

What is meant by anonymisation and pseudonymisation?

As mentioned above, the GDPR only applies to data that contains information that relates to an identifiable person. If data is truly anonymised, then it no longer refers to an identifiable person and thus can be processed without restriction. While the GDPR does not provide a definition of anonymisation, Recital 26 states the following two conditions:

- *To determine whether a natural person is identifiable, account should be taken **of all the means reasonably likely** to be used, such as singling out, either by the controller or by another person to identify the natural person **directly or indirectly**.*

- *To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all **objective factors**, such as the **costs** of and the **amount of time** required for identification, taking into consideration the **available technology at the time** of the processing **and technological developments**.*

The notion of *reasonably likely* is not strictly defined although the UK's Information Commissioner's Office (ICO)[15] provides the guidance of considering what would be reasonably likely for a *determined* person (which could be an investigative journalist, criminal or industrial spy (e.g.)).

Pseudonymisation on the other hand is a process of de-identification of data but the data is not fully anonymised. Article 4 defines pseudonymisation as the following:

"'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

Some research even goes further and attributes a difference between pseudonymous data and strongly pseudonymous data[16] with the latter making it significantly more difficult to reverse engineer the pseudonymisation process and re-identify the person; however, it is not complete anonymisation.

Who are the controllers and processors?

Processing of personal data can be carried out by individuals, authorities, agencies and other bodies as either a data controller or a data processor. Regardless of their status, both controllers and processors' activities fall under the GDPR.

*A **'controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing of personal data**; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."*

*"A **'processor'** means a natural or legal person, public authority, agency or other body which **processes personal data on behalf of the controller.**"*

[15] ICO (n.d.) Can we identify an individual indirectly from the information we have (together with other available information)? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/can-we-identify-an-individual-indirectly. (last accessed 2 April 2021)

[16] Hintze, M. and El Emam, K., 2018. Comparing the benefits of pseudonymisation and anonymisation under the GDPR. Journal of Data Protection & Privacy, 2(2), pp.145-158.

2.2.1. Core principles of data protection

Chapter 2 of the GDPR sets out the core principles in relation to the processing of personal data. In particular, this section will focus on the specific principles (Article 5); lawfulness (Article 6); consent (Article 7); and the additional requirements that govern the processing of special categories of personal data.

Different components of the 7SHIELD system may process personal depending on their implementation, the main components that will process personal data include the following.

- System user data including that linked to secure authentication mechanisms.
- Acquisition of online data when searching from threat intelligence.
- Image and video data obtained from CCTV, drones and other video surveillance cameras.
- Images required to apply facial recognition technology.
- Health data collected from wearables worn by first responders.
- Personal data linked through advanced modelling techniques.
- Data collected using social media services to communicate with citizens.

In addition, personal data will be collected for research purposes. This is considered separately in Section 6.

2.2.1.1. Article 5 – Principles relating to the processing of personal data

Article 5 sets out the main conditions for compliance with the GDPR and applies in all situations where personal data is processed and to all data controllers and data processors. Therefore, all processing of personal data within 7SHIELD must comply with these principles and the data controller must be able to demonstrate this compliance. The six core principles mean that personal data should be processed according to the following (as set out in Article 5, emphasis ours):

- *processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency**').*
- *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('**purpose limitation**').*
- *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **('data minimisation')**.*

- *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**accuracy**').*
- *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('**storage limitation**').*
- *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity and confidentiality**').*

Each of these six core principles will be at the heart of all 7SHIELD activities that interact with personal data and the corresponding technological components will use this initial version of the framework to identify all their requirements with respect to the GDPR and refine their approaches to data processing. D2.6 will build upon the work in this deliverable to include detailed coverage of how compliance with data protection aspects was achieved for each component and the system as a whole.

2.2.1.2. Article 6 – Lawfulness of processing

For each act of data processing a legal basis within law must be established in order to carry out that processing. The GDPR, under Article 6, foresees six different appropriate legal bases for processing.

- Consent*: the data subject has given consent to the processing of his or her personal data for one or more specific purposes.*
- Performance of contract: *processing 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.*
- Legal obligation: *processing is necessary for compliance with a legal obligation to which the controller is subject.*
- Vital interests: *processing is necessary in order to protect the vital interests of the data subject or of another natural person.*
- Public interest: *processing 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.*

- **Legitimate interest:** *processing 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.*

Within 7SHIELD, as a project, the expected lawful basis for processing will depend on each organisation and the specific context. During the project and the associated research activities (e.g., workshops and piloting activities), 7SHIELD will recruit only known participants and thus the lawful basis for processing will be consent (specifically informed consent). Although such recruits will likely be from the organisations arranging the piloting activities, no person or employee will be under any obligation to participate and must volunteer freely without consequence. More details on the approach and obligations in the recruitment of research participants can be found in D9.1.

In other instances, for example, research institutions may rely on Public Interest whereby research is part of the mandate of the organisation.

In the operational version of the system, legitimate interest may form the legal basis where it is essential for the operator to process such data to protect the GS and the associated infrastructure. It is the responsibility of each organisation to establish the legal basis for the specific activities they carry out involving personal data.

2.2.1.3. Article 7 – Conditions for consent

The majority of the research in 7SHIELD that entails data processing should have its legal basis established through the form of consent. For example, data collected relating to user requirements or piloting activities will recruit volunteers (most likely from within the consortium) to participate in workshops or testing events. In these cases, all participants will give their consent for their personal data to be processed in relation to the activities within the project.

The GDPR sets outs several requirements in Article 7 that provide specific conditions for obtaining and managing participants' consent. This include the requirement for the controller to demonstrate that the data subject has given their consent and, if they have done so via a written declaration, the controller has ensured that the request for this consent has been in a clear manner that is distinguishable from any other aspects. Recital 32 sets outs the conditions for consent stating that it should be *'freely given, specific, informed and unambiguous'* and by Recital 42 it must be ensure that participants are able to refuse or withdraw consent without detriment.

Deliverable 9.1 has already covered in detail the processes for the recruitment of participants to be involved in various 7SHIELD project activities (participation in workshops, participation in piloting activities, and similar).

The GDPR sets out a number of rights for the data subject in Chapter 3. These, amongst others, cover right of access (Article 15) which includes the data itself and the details of the processing activities, the right to rectification (Article 16) should the data subject consider the data held by the processor as inaccurate, the right to be forgotten / the right to erasure (Article 17) that allows data subjects to request their data is erased.

In the research aspects such as participating in piloting activities these are set out in the information provided to participants in advance of any activities. These are set out in D9.1

2.2.1.4. Article 9 - Processing of special categories of personal data

In 7SHIELD there are tasks which involve the processing of data in relation to performing activities such as facial recognition and the processing of data collected from wearable sensors. Such data may constitute as biometric data or health data and thus fall under special categories of personal data. In order to process such data, the GDPR sets out a number of further conditions to ensure that the rights of the data subject are protected. Therefore, the processing of such data should only take place if one of the conditions in Article 9(2) applies.

In the case of 7SHIELD, the most likely bases are **explicit consent** (9(2)(a)) given by the data subject – for example this is most likely to apply in testing and the piloting activities where the data subjects are clearly known to the researchers and are able to freely and independently give their consent and in the operational system concerning persons who would wear the sensors. In the operational version of the 7SHIELD system the condition for **substantial public interest** may apply depending on national legislation (9(2)(g)) while in the project the condition in 9(2)(j) specifically relates to **scientific or historical research purposes** provided it is in accordance with Article 89(1) based on Union or MS law (specific considerations for MS are discussed in Section 6.1).

2.2.1.5. Automated decision-making and profiling

7SHIELD is developing a system to enhance the safety of security of GS. 7SHIELD will make use of advanced technological processes such as machine learning and artificial intelligence (AI). When making use of such technology, it is necessary to consider how outputs from automated processing are used. In this context, Article 22 of the GDPR states that a data subject should '*not be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning … or significantly affecting him or her.*'

Activities within 7SHIELD have no intention with 7SHIELD to profile or make automated decisions about specific data subjects. Where data is initially processed in an automated manner, the 7SHIELD system makes a provision for a human-in-the-loop or a review of outputs before any decision are made. 7SHIELD will take a data protection by design and

default approach (as set out in Article 25) and extensive security, legal and ethical requirements for part of the user requirements elicitation process.

2.2.1.6. Data protection impact assessments

Data protection impact assessments (DPIA) are required when processing of personal data could be considered as high-risk based on a number of specific circumstances as set out in Article 35 of the GDPR. Of particular relevance to 7SHIELD are the occasions where a DPIA could be required due to the high-risk nature of the processing activity. Deliverable 9.4 already identifies where a DPIA is required for the activities in the 7SHIELD project. Although 'high-risk' is not explicitly defined the use of new technologies to process data is of particular importance. It may also be considered necessary in case of systematic monitoring or large-scale processing.

In D2.6, we will build on the individual DPIAs for individual components in the context of the 7SHIELD project and look to complete a DPIA for the entire system to ensure all possible flows of personal data are considered and managed.

2.3. Relevant legislation for 7SHIELD domain

While the protection of fundamental rights and the application of the GDPR are two essential pieces of legislation within the context of 7SHIELD, there is a range of legislation relating to the specific domain of 7SHIELD (i.e., the protection of CI, operation of GS, cybersecurity), and the technology used within 7SHIELD itself that are also subject to a range of legislation to ensure their proper use and application.

2.3.1. Protection of national critical infrastructure

In 2008, the European Council published Council Directive 2008/114/EC[17] on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. This directive provides a procedure for identifying European Critical Infrastructures (ECIs); however, its main focus was on the energy and transport sectors, albeit with a look ahead to the need to include other sectors, in particular, information and communication technology. The directive itself emphasises that it is the responsibility of the MS and the owners of the CIs to ultimately protect them. Nonetheless, the directive identified the need for a common procedure to identify CIs and determine their security requirements. The directive also set out the need for Operator Security Plans (OSPs) and Security Liaison Officers (SLOs) which contain the security solutions required for a particular piece of CI while the SLO provides a single point of contact to manage the interaction between the owner/operator of the CI and the MS authority.

[17] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Official Journal L345, pages 75-82. 23 December 2008. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2008:345:TOC

The 2008 directive committed to a review in 2012 of the directive and the associated European Programme for Critical Infrastructure Protection (EPCIP). The publication of this review[18] found that MS with relatively mature CIP programmes did not achieve significant added value from the directive; however, other MS with less mature CIP benefited more greatly. Overall, though, the perception was that there had not been tangible improvements to the security of ECI.

In 2018, the EC launched a further evaluation of the 2008 directive which also included a public consultation on the evaluation. The initial results of this evaluation led to the EC adopting an inception impact assessment roadmap[19] on CIs that will aim to address the following aspects, all of which are relevant to the 7SHIELD implementation.

- *Discrepancies in implementation of the ECI Directive and disparities in the level of CIP.*
- *Increased interdependencies and related risks of cascading effects across sectors.*
- *Insufficient focus on resilience of critical infrastructure at the European level.*
- *Varying risk assessment methodologies and co-ordination and response mechanisms.*[20]

Following this, in late 2020, the EC introduced a proposal for a directive (COM (2020) 829) on the resilience of critical entities,[21] aligning the proposed directive with the EU 2020 Security Union Strategy.[22] Crucially for 7SHIELD, this means it now directly includes space infrastructure as one of the ten named CIs (others are energy, transport, banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, and public administration). Secondly, and also equally relevant for 7SHIELD, is the proposal for common criteria for national risk assessments to identify critical entities as well as additional obligations on MS CIs that have European significance (those which provide CI to more than one third of MS). The proposal also sets out synergies with the similarly proposed NIS2 (Network and Information Systems) Directive, which is discussed in the next section. The proposal also notes the potential impact on fundamental rights highlighting that it would "*enhance the resilience of critical entities providing essential services [… therefore*

[18] EC (2012) Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP) SWD (2012) 190 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/pdf/policies/crisis_and_terrorism/epcip_swd_2012_190_final.pdf

[19] EC (2020) Protecting critical infrastructure in the EU – new rules https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12462-Enhancement-of-European-policy-on-critical-infrastructure-protection

[20] Practical Law EU (2020) European Critical Infrastructures: European Commission adopts inception impact assessment Roadmap on critical infrastructures. Thomson Reuters Practical Law. 23 June 2020. https://uk.practicallaw.thomsonreuters.com/w-026-1575

[21] Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities COM/2020/829 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN

[22] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy COM/2020/605 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605

…] the overall risk for disruptions at both the societal and individual level would be reduced [… and *…] could contribute to ensuring a higher level of public security*".

Alongside, specific directives on the CIP runs the Policy on Critical Information Infrastructure Protection (CIIP)[23], this communication was initially adopted in March 2009[24] to protect Europe from cyber disruptions based on five pillars:

- Preparedness and prevention
- Detection and response
- Mitigation and recovery
- International cooperation
- Criteria for ECIs in the field of ICT.

This approach was strengthened in 2011[25], and in 2012 a European Parliament Resolution on CIIP towards global cyber security[26]. This was then taken forwards as part of the NIS Directive discussed further in Section 2.3.3 below.

2.3.2. Space ground segments

Ground segments of space systems are an integral part of the overall infrastructure for a satellite operation. Much of the European legislation places a greater emphasis on the operation of the satellites as opposed to the operation of the GS. In the space sector, the most recent proposal from the EC that looks at harmonising the EU space programme is the 2018 proposal[27] for establishing the 'EU Agency for the Space Programme' taking over from the current European Global Navigation Satellite Systems Agency (GSA). In December 2020, an agreement was reached between the European Parliament and the EU MS to approve the space programme, thus bringing all EU space activities under a single

[23] EC (2013) Policy on Critical Information Infrastructure Protection (CIIP) https://ec.europa.eu/digital-single-market/en/news/policy-critical-information-infrastructure-protection-ciip

[24] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" {SEC(2009) 399} {SEC(2009) 400} /* COM/2009/0149 final */https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

[25] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security' /* COM/2011/0163 final */ https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF

[26] European Parliament resolution of 12 June 2012 on critical information infrastructure protection – achievements and next steps: towards global cyber-security (2011/2284(INI)) https://www.europarl.europa.eu/doceo/document/TA-7-2012-0237_EN.html

[27] EC (2018) EU budget: A €16 billion Space Programme to boost EU space leadership beyond 2020. 6 June 2018 https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4022 (last accessed; 22 April 2021)

umbrella[28,29]. This programme includes further support for the Galileo and EGNOS (European Geostationary Navigation Overlay Service) satellite navigation systems as well as the Copernicus DIAS (data and information access services). ONDA DIAS[30] (which forms the piloting for PUC5) builds upon the Copernicus platform to allow users to host data and build cloud applications.

Within the space sector, ESA (the European Space Agency) has developed the European Centre for Space Law (ECSL) that brings together researchers and organisations involved in the regulation of space; however, the majority of its outputs relate either to outer space or concern ESA directly.

Within the 7SHIELD piloting activities, the organisations involved are linked to a range of EU space infrastructure services including:

- NOA's operation of Copernicus Sentinel Data Hubs
- The collaboration between SPACEAPPS and ESA on the ICE Cubes Services
- Serco's ONDA DIAs platform which is once of ESA's five DIAS linked to the Sentinel's satellites and Copernicus.

Briefly, we discuss relevant aspects of the legislation related to ESA, Copernicus, and the Sentinels. **ESA** or the European Space Agency was established in 1975 under the convention for the establishment of a European Space Agency[31] to promote cooperation between European States in space research and technology. **Copernicus** is the Earth observation programme of the EU and is partnership between the European Commission and ESA. The conditions for the Copernicus programme[32] are that it should provide users with free, full and open access to the Copernicus Sentinel Data and Service Information[33]. Therefore, the provision of such services through the ground segments should ensure that this goal is upheld. The **Sentinels[34]** are Copernicus's space missions, each with a different purpose providing specific data.

[28] EC (2020) Commission welcomes the political agreement on the European Space Programme. 16 December 2020 https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2449 (last accessed; 22 April 2021)

[29] Commission Staff Working Document Impact Assessment accompanying the Document Proposal for a Regulation of the European Parliament and of the Council establishing the space programme of the Union and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013, (EU) No 377/2014 and Decision 541/2014/EU SWD/2018/327 final - 2018/0236 (COD) https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52018SC0327

[30] ONDA DIAS (2018) ONDA DIAS. ONDA by Serco https://www.onda-dias.eu/cms/ (last accessed; 22 April 2021)

[31] ESA (n.d.) Convention for the Establishment of a European Space Agency https://www.esa.int/About_Us/Corporate_news/Articles

[32] Regulation (EU) No 377/2014 of the European Parliament and of the Council of 3 April 2014 establishing the Copernicus Programme and repealing Regulation (EU) No 911/2010. Official Journal L122, pages 44-66. 24 April 2014. http://data.europa.eu/eli/reg/2014/377/oj

[33] Commission Implementing Decision (EU) 2018/621 of 20 April 2018 on the technical specifications for the Copernicus space component pursuant to Regulation (EU) No 377/2014 of the European Parliament and of the Council. Official Journal L102, pages 56-79. 23 April 2018. http://data.europa.eu/eli/dec_impl/2018/621/oj

[34] ESA (2021) Sentinels Online. https://sentinels.copernicus.eu/web/sentinel/home (last accessed; 22 April 2021)

2.3.3. Cybersecurity

The security of the ground stations associated with satellite systems has recently been brought into focus by the Head of Security at GSA who noted that "with stations spread across the globe, we need to ensure that these are not targets of malicious attacks" and that it is necessary not only to protect critical infrastructure, but also the information that the sites contain[35]; therefore, placing an even greater emphasis on the need for robust cyber security operations at ground segments.

Within Europe, there are two main pieces of cybersecurity legislation: the NIS Directive and the Cybersecurity Act.

The NIS Directive[36], more formally known as the Directive on security of network and information systems was the first piece of EU wider legislation focused on cybersecurity. The goal of the directive was to 'boost the overall level of cybersecurity in the EU.'[37] The directive itself had five main purposes as set out in Article 1.

a) *To lay down obligations for all Member States to adopt a national strategy on the security of network and information systems.*

b) *To create a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them.*

c) *To create a computer security incident response teams network ('CSIRTs network') in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation.*

d) *To establishes security and notification requirements for operators of essential services and for digital service providers.*

e) *To lay down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems.*

In relation to 7SHIELD and the operation of CI, point (d) in the above is explicitly relevant. Article 5 of the directive sets out a process for identifying operators of essential services (OES). Articles 15 and 16 then set out the security requirements that must be put in place by operators of such services. These measures are designed to align with the requirements set out in the legislation relating to the operation of critical entities as described in Section 2.3.1 above. These requirements are divided into 'Security requirements and incident

[35] GSA (2021) Agile governance needed for secure space systems. 30 March 2021 https://www.gsa.europa.eu/newsroom/news/agile-governance-needed-secure-space-systems (last accessed: 10 April 2021)

[36] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Official Journal L194, pages 1-30. 19 July 2016. http://data.europa.eu/eli/dir/2016/1148/oj

[37] EC (2021) NIS Directive https://ec.europa.eu/digital-single-market/en/directive-security-network-and-information-systems-nis-directive (last accessed: 23 April 2021)

notification' (Article 14) and 'Implementation and enforcement' (Article 15). To prepare for and during the response to an incident OES must do the following (paraphrased).

- Take appropriate and proportionate technical and organisation measures to manage the risks posed to the security of the NIS in the operations.
- Take appropriate measures to prevent and minimise the impact of any incidents.
- In the case of an incident, notify the appropriate CSIRT (Cyber Security Incident Response Team) or competent authority.
- Consider the number of users affected, duration and geographical spread of those affected by the incident.

Furthermore, once informed of an incident CSIRTS must inform CSIRTs of any other affected MS and the CSIRT may also inform the public where necessary.

With respect to Article 15, the legislation then enables MS to give their competent authorities the powers to assess and access the information necessary determine the compliance of OES with their obligations.

To support the implementation of the directive the Commission also developed the 'NIS Toolkit' (COM 2017 (0476))[38] which contains best practice advice for implementing aspects of the directive.

Within the NIS Directive, it was foreseen to include a provision to review the consistency of the approach taken by MS in their identification of OES and to, in general, review the functioning of the directive. Based on this review, in December 2020 a proposal for a revised NIS Directive (NIS2)[39] was made by the Commission based on the ever-evolving digital landscape. This revised directive also goes hand-in-hand with the proposed directive on the 'resilience of critical entities' (COM (2020) 829) to ensure the digital infrastructure is considered equally with physical infrastructure.

In terms of the security and resilience of critical infrastructure, the review of the NIS Directive noted the discrepancies between different MS in designating entities as OES and thus led to differences in implementation.[40] Specifically relevant for 7SHIELD is the explicit inclusion of the space sector as a key infrastructure within Europe[41].

[38] Communication from the Commission to the European Parliament and the Council Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. COM/2017/0476 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0476

[39] EC (2020) Proposal for directive on measures for high common level of cybersecurity across the Union. 16 December 2020. https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

[40] Proposed directive on measures for a high common level of cybersecurity across the Union https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72166 (last accessed: 20 April 2021)

[41] Annex to the Proposed directive on measures for a high common level of cybersecurity across the Union https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72172 (last accessed: 20 April 2021)

Similar to the NIS Directive, the proposed NIS2 specifies actions required for the management of cybersecurity risks in Article 18. These include the following (paraphrased) that are currently of most relevance to 7SHIELD.

- Take appropriate and proportionate technical and organisation measures to manage the risks posed to the security of the NIS in the operations including:
    - Risk analysis and security policies
    - Incident handling
    - Business continuity and crisis management
    - Supply chain security
    - Security in the acquisition, development of maintenance of NIS; vulnerability handling and disclosure
    - Procedures for testing risk management measures
    - Use of cryptography and encryption.
- Take into account the specific vulnerabilities relevant to each supplier in the supply chain including their quality and cybersecurity practices.
- Take all necessary measures if gaps in compliance are identified to rectify without undue delay.

As with the NIS Directive, organisations will still be required to report incidents to CSIRTS (Article 20) and tying up with the 2018 Cybersecurity Act (discussed below), organisations may need to demonstrate compliance with specific European cybersecurity certification schemes (Article 21).

The 2018 Cyber Security Act[42] also acknowledges the role that cybersecurity has to play in the protection of critical infrastructure and, alongside promoting the role of ENISA, it puts forward the need to establish a European cybersecurity certification scheme to assists in harmonising approaches to cybersecurity. ENISA (European Union Agency for Cybersecurity) will support the identification of OES that provide ECI while the act makes provisions for the possibility that the certification frameworks identified could become mandatory for certain OES. Aspects around cybersecurity and standardisation will be covered in more depth in D2.5.

[42] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) Official Journal L151, pages 15-69. 7 June 2019. https://eur-lex.europa.eu/eli/reg/2019/881/oj

3. Legal considerations for 7SHIELD technology

The goal for 7SHIELD is to develop a system that enhances the safety and security of space systems, specifically focused on ground segments. The framework for 7SHIELD divides the components of the system in four categories: prevention technologies, detection technologies, response technologies and mitigation technologies. In this section, we cover the main legal aspects relating to the technologies developed within 7SHIELD for each of these categories. In some instances, for example, the use of drones, these are used for more than one purpose within the project; therefore, we discuss the legal aspects related to the deployment of these technologies in only one category. Figure 1 below shows the overall structure of the 7SHIELD project as a reference for how 7SHIELD proposes to develop technology to address each category.

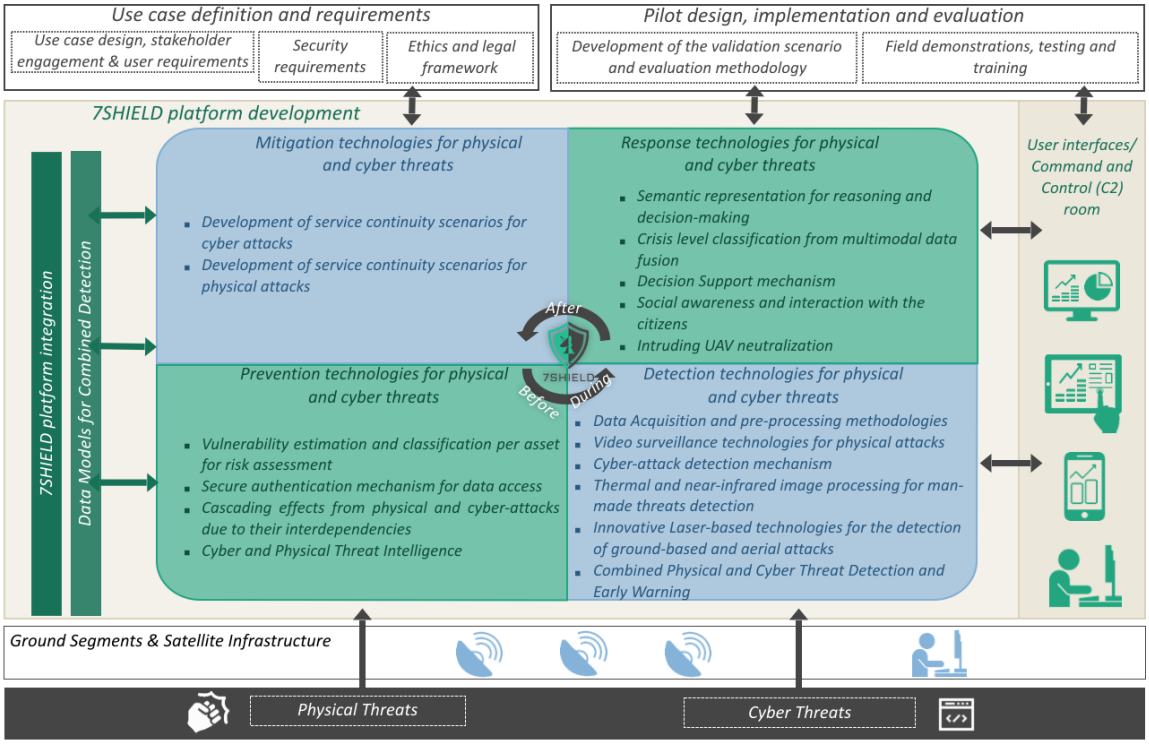

Figure 1: Framework for 7SHIELD demonstrating the proposed technologies and different aspects of the system (retrieved from https://www.7shield.eu/concept/)

3.1. Prevention technologies

At the heart of all safety and security activity, is implementing a robust plan and mechanisms to prevent security incidents happening at all. 7SHIELD proposes several mechanisms for improving the resilience of a GS to an attack.

- Risk assessment tools
- Secure authentication mechanism
- Combined threat assessment tool

- Cyber and Physical Threat Intelligence

The legal aspects relating to the first three of these are discussed in this section while the aspects relating to acquisition of cyber and physical threat intelligence are covered in Section 3.2.1.

3.1.1. Risk and vulnerability assessments

Vulnerability assessments, and wider risk assessments are an important part of managing CI. Vulnerabilities can be associated with physical, cyber or human factors, and, in reality, are likely to be exposed via a combination of these factors. The latest proposed directive on the resilience of critical entities[21] makes specific provisions for MS to carry out risk assessments to identify and subsequently monitor risks associated with critical entities (Article 4) while the critical entities themselves should also regularly assess risks based on agreed national frameworks as well as other relevant information (Article 10).

While COM(2020)829 has not completed the legislative procedure in which it will become EU law it is prudent for MS and operators of ECI to be aware of the forthcoming requirements to ease compliance at a later date.

Article 4(1) includes the following requirements that may be relevant to 7SHIELD in carrying out risk assessments. Firstly, the proposed directive indicates that the following risk areas should be included in the assessment.

*"The risk assessment shall account for all relevant **natural and man-made risks, including accidents, natural disasters, public health emergencies, antagonistic threats, including terrorist offences**…"*

For entities themselves carrying out the risk assessment the proposal sets out the need for critical entities to take appropriate measure to ensure resilience (Article 11(1)). These are presented below, and organisations can work backwards to identify where potential vulnerabilities could be identified.

a. *prevent incidents from occurring, including through **disaster risk reduction** and climate adaptation measures.*
b. *ensure **adequate physical protection of sensitive areas**, facilities and other infrastructure, including fencing, barriers, perimeter monitoring tools and routines, as well as detection equipment and access controls.*
c. *resist and mitigate the consequences of incidents, including the implementation of risk and **crisis management procedures** and protocols and alert routines.*
d. *recover from incidents, including **business continuity measures** and the identification of alternative supply chains.*
e. *ensure adequate **employee security management**, including by setting out categories of personnel exercising critical functions, establishing **access rights** to*

sensitive areas, facilities and other infrastructure, and to sensitive information as well as identifying specific categories of personnel in view of Article 12[43].

f. *raise awareness about the measures referred to in points (a) to (e) among relevant personnel.*

3.1.2. Secure authentication

The NIS Directive[44] concerns OES, i.e., CIs. Article 14(1) of the directive states:

"Member States shall ensure that operators of essential services take appropriate and proportionate ***technical and organisational measures to manage the risks*** *posed to the security of network and information systems which they use in their operations."*

Alongside the publication of the directive was a reference document that identifies security measures for OES[45]. Within this document are considerations both for the IT Security Administration and Identity and Access Management requirements. Within this, systems are expected to implement the following:

- **Identification** through assigning unique accounts to users and automated processes that are regularly reviewed.
- Use of an **authentication mechanism** that have been changed from the default credentials.
- **Access rights** that utilise the principles of **need-to-know** and **least privilege** that are reviewed at least yearly to ensure they are providing access only to the functionalities necessary.

In addition to the directive and the associated reference guide and the NIS Toolkit, ENISA has also published a companion that details the minimum-security measures for operators of essential services[46] that maps the security measures required to the three main standardisation frameworks (ISO27001, NIST CSF, ISA/IEC 62443).

Given that many of these systems hold personal data the implementation of secure authentication mechanisms provides technical measures that protect and limit access to personal data within the system thus increasing compliance and resilience to unauthorised access to such data. The need for such technical (along with organisational) measures is

[43] Article 12 relates to background checks for personnel.
[44] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148
[45] NIS Cooperation Group (2018) Reference document on security measures for Operators of Essential Services. February 2018. https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_security_measures_0040C183-FF20-ECC4-A3D11FA2A80DAAC6_53643.pdf
[46] ENISA (n.d) Minimum Security Measures for Operators of Essentials Services. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services (last accessed: 21/04/2021)

necessitated by Article 32 of the GDPR (on the security of processing) and requires organisations to implement levels of security appropriate to the risk.

3.1.3. Cascading effects (& prevention of)

One of the key core outcomes of the review of 2008/114/EC[17] that fed into the COM (2020) 829[21] proposal was the lack of consideration for the impact of cascading effects resulting from an incident on one installation of critical infrastructure onto other sectors. The recognition of these interdependencies and the need to have plans to prevent, counteract and mitigate against them are essential. Furthermore, a greater consideration of cross-border interdependencies is also becoming more prominent and, given the context of 7SHIELD, the wide use of space systems makes this a significant consideration.

Specific regulations that may apply to the prevention of cascading effects include the proposed Article 13 on incident notification in COM(2020)829 that require operators of critical entities to inform the competent authorities if an incident is likely to cause significant disruption. Such information should include number of affected users, anticipated duration and the geographical area disrupted (matching the requirement in the proposal for NIS2). While this proposal is not currently implemented it is important for operators of critical entities to consider how they will communicate potential incidents and mitigate against cascading effects. 7SHIELD includes research that will identify how best to communicate with citizens and other stakeholders in the event of an incident.

3.2. Detection technologies

Within 7SHIELD, detection technologies are focused on detecting unauthorised access to the ground segment either through direct physical access to the GS site or to the information systems via a cyber-attack. Detection methods fall into two modes of monitoring: proactive monitoring that scan the environment for potential future threats; and reactive monitoring that detect when someone has already gained access (either physically or digitally). In some cases, certain technologies can be applied in both situations. Such methods of detection activities and the use and application of the technologies that underpin them are subject to numerous legislation which we will review in this section. The main components that are included in 7SHIELD's detection technologies include the following.

a) Data collection and edge processing

b) Face detection and face recognition

c) Video-based object and activity recognition

d) Cyber-attack detection framework

e) Thermal and near-infrared image processing for man-made threats detection

f) Detection of ground based and aerial intruders

g) Combined cyber-physical threat detection, early warning, and geospatial event correlator.

In terms of legal considerations data collection activities (a) are discussed in Section 3.2.1, while the legal requirements pertaining to the safety of drone deployment are discussed in the next Section (3.3.4), video surveillance in Section 3.2.2 covers all aspects of (b), (c), and (e).

3.2.1. Online data acquisition

Information posted online may range from specific threats discussing an attack to the availability of information that could be used to better understand the security environment of a GS to computer code that may facilitate cyber access to the GS information systems. Identifying the presence of this information online could be vital to the prevention of an attack. Open-source locations where such information could be found ranges from social media sites and forums, other specialist surface and deep web sites as well as on the dark web.

In legal terms, the main issues with web-scraping and access of internet data relate to whether the data contains personal data or whether the information being scraped is copyrighted. A further grey area exists between what is legal and what is ethical concerns the potential infringement of the owners' terms of service (particularly for services accessed through APIs) or in some cases of web scraping the adherence to the robots.txt file.

3.2.1.1. Data privacy

As discussed extensively in Section 2.2 above, the GDPR sets out the requirements for the processing of personal data. Access of data from social media services, web forums and other sites may contain personal data. In most cases, informing the data subject that their data is being processed both during the acquisition process and afterwards is either unfeasible and/or would alert the data subject they are considered a potential threat. Furthermore, it is unlikely that only personal data relating to individuals who pose a threat would be processed due to the nature of online data collection that increases the likelihood of collateral intrusion (the collection of data about persons who are not the target of the inquiry).

Therefore, in the process of acquiring online data specific measures should be taken to limit or eliminate the collection of personal data or explicit justification and a legal basis in law for such data processing should be established in advance and a data privacy impact assessment (DPIA) conducted prior to any collection activities to ensure that any risks relating to data processing are identified and appropriately mitigated against. In particular, this type of collection of data in some cases could be considered as systematic monitoring and/or large-scale data processing under Article 35 which determines the requirements for a DPIA.

3.2.1.2. Copyright

Information posted on many websites may be subject to copyright either by the site themselves or by sites that host user generated context also by those users. Downloading such content may result in the infringement of copyright depending on the planned use of such content once it has been accessed. The EU enacted the "Copyright Directive" (2019/790)[47] which should be transposed into law by MS by 7 June 2021. The directive provides an exception for text and data mining for the purposes of scientific research (Article 3) which would be appliable within the 7SHIELD project but not the implementation of the system itself.

Given there is no intention to republish information accessed from online sites within 7SHIELD copyright is likely not a significant concern; however, it is important that developers of technologies that acquire online data are aware of subsequent uses of that data by other parts of the system and that copyright is not infringed.

3.2.1.3. Terms of Service

Many websites and, especially social media services, that require users to sign up to access data through APIs (application programming interfaces) have associated terms of service that may restrict who can use the APIs, what purposes they use it for, the frequency that they can make requests and the amount of data that be retrieved. Terms of Service are generally considered to be legally binding as the user has likely agreed to abide by such conditions on sign up to a service.

Therefore, if the technologies for data acquisition within 7SHIELD make use of APIs then it is necessary to comply with their terms of service. While not the focus of 7SHIELD, users of such services should be reminded that social media APIs often explicitly forbid the use of APIs for law enforcement and surveillance purposes.

3.2.1.4. Robots exclusion protocol

The robots exclusion protocol (REP), more commonly known as robots.txt is a web standard specifically designed to communicate with web crawlers and scrapers to instruct them on which parts of a website can be scraped and which cannot. Robots.txt is a web standard (albeit not an official one) rather than a legal requirement. The Robots.txt file generally includes which areas of a website can be scraped and which cannot as well as including settings such as the crawl delay which limits how often a crawler can access this site and prevents the issues presented below.

While many websites are set up to cope with thousands and even millions of hits at any one time, smaller sites may not have the infrastructure to cope with multiple requests over a short period of time. By its nature web crawling or scraping usually requires traversing a site

[47] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market (the "Copyright Directive" https://eur-lex.europa.eu/eli/dir/2019/790/oj

far faster than a person navigating the site could alone. If a site is unable to cope with higher-than-normal volumes of traffic, then crawling the site may severely degrade the site's performance or cause it to go down altogether. Excessively accessing a site in such a manner could be construed by the site's owners or operators as a denial-of-service attack and lead, for example, to consequences such as the banning of IP ranges or in more severe cases reporting to authorities.

3.2.2. Video surveillance

Video surveillance, and particularly what is done with the video footage after it has been collected is a prominent topic within the security domain. In this section, we discuss the legal frameworks around the methods of collection while Section 3.2.3 covers in more detail the computational processing of such data.

The purpose of video surveillance is to monitor a specific area for the presence of potential security incidents which may include unauthorised access, criminal or other nefarious activity, or the ability to review the footage at a later date following an incident. Cameras are not only deployed to collect standard video footage; thermal and infrared imaging can also be deployed as alternate monitoring methods. Such cameras can be deployed statically, be controlled by human operators, or be attached to drones or other autonomous vehicles to monitor a wider area.

CCTV or closed-circuit television is routinely deployed in both public and private spaces across Europe (and the world).

A concern relating to data protection is that CCTV footage can be used to identify natural persons (often when combined with other information) and thus adherence to the principles of GDPR is essential. The European Data Protection Supervisor (EDPS)[48] lists some best practices for the use of video surveillance which include the following (although these were originally aimed at EU institutions the overall principles are more widely applicable).

- Ensuring high data quality through the application of the data minimisation principle by intelligent deployment of cameras focused on specific known security problems.
- Making information about collection known (including the purpose, retention and who has the footage) to those whose data might be collected.
- Maintaining a detailed policy on the length of data retention period and when such footage is deleted.

In particular, in the 7SHIELD system if staff working at the site are likely to be captured through the CCTV used for security monitoring, they must be informed that such data capture is taking place.

[48] EDPS (n.d.) Video Surveillance. European Data Protection Supervisor. https://edps.europa.eu/data-protection/data-protection/reference-library/video-surveillance_en (last accessed: 6 April 2021)

Similarly, if footage is being collected from drones with cameras attached then those on site should be informed that such data collection is taking place.

7SHIELD also proposed to make us of thermal and infrared imaging cameras for better detection. While thermal imaging can come under scrutiny if it has been used to take temperatures (as we have seen with the COVID-19 pandemic) and thus is a form of health data associated with a particular individual, using thermal or infrared data to detect the presence of a live human (or mammal) without identifying them raises far fewer concerns.

3.2.3. Processing image and video data

In 7SHIELD, the capture of image and video data is the first step in a semi-automated process that also includes in the first instance object and activity detection and in a second instance potentially facial recognition. The European Data Protect Board (EDPB) published guidelines in 2019 on the processing of personal data through video devices.[49]

3.2.3.1. Object and person detection

In case of a physical intrusion, 7SHIELD proposes to use video streams to detect the presence of a person, animal or object (such as drones). The detection of objects, animals or persons in a video stream do not generally raise legal concerns provided the person cannot be identified from the video stream. If a person is identifiable then such processing becomes the processing of personal data and is subject to the GDPR.

Activity detection is a form of automated processing that aims to deduce what activity the detection object/person/animal is currently doing. A simple example for a person could be the distinctive actions of walking, running, crouching, or crawling. The identification of such behaviours or activities do not raise legal concerns; however, should such data be used to infer whether such an activity is suspicious or not this could be considered as automated profiling within the GDPR (if the person is identifiable) and therefore specific constraints should be in place to monitor such decision-making alongside a human-in-the-loop to review any output before an action is taken based on the output of the analysis.

3.2.3.2. Facial Recognition

The legal and ethical issues concerning facial recognition systems is one of the most prominent topics in the application of AI in the 21st century. Facial recognition systems by their very nature process personal data and thus are subject to all the provisions of the GDPR as well as the ECHR, particularly Article 8 (respect for private and family life). Facial recognition technology is considered as processing biometric data for the purposes of identification and is therefore considered a special category of personal data. In addition,

[49] EDPB (2019) Guidelines 3/2019 on processing of personal data through video devices. European Data Protection Supervisor. 10 July 2019. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf (last accessed: 21 April 2021)

by definition the process of facial recognition must require the operator to also maintain a database of faces to which other faces can be matched. Therefore, the processing of this additional data must also be considered which is where technologies such as Clearview AI raise significant legal concerns (as demonstrated by this response from the European Data Protection Board (EDPB)[50]) due the perceived indiscriminate use of mass collection of facial data to construct their comparison database. While the persons to be matched against will be tightly controlled within the preparation and piloting activities within the 7SHIELD project, careful consideration of how such a technology could deployed operationally will be reviewed in depth in D2.6

The Council of Europe has also recently issued Guidelines on the use of Facial Recognition[51] including specific considerations when identifying a legal framework to ensure the lawfulness of the processing. These are detailed explanations of the specific use and purpose, reliability and accuracy of the algorithms used, duration of the retention of any photos, auditing of the previous criteria, traceability of the process and the safeguards in place.

Facial recognition also raises many ethical issues in particular relating the ways in which they are trained using AI models which are addressed extensively in Section 5.2.

3.3. Response technologies

In 7SHIELD, response technologies are focused on addressing and responding during and in the immediate aftermath of an attack. Methods such as (a) and (b) are focused on data processing, semantic modelling and classification of incidents to speed up response, (c) makes use of wearables to monitor through sensors various health aspects of first responders, (d) is focused on communicating with citizens and understanding data from social media, while (e) focuses on technical to neutralise drones that are potentially entering the GS site.

a) 7SHIELD Knowledge Base

b) Crisis classification module

c) Tactical decision support system

d) Social awareness and warning message generation

e) Drone neutralisation mechanism

[50] EDPB (2020) EDPB response to MEPs Sophie in 't Veld, Moritz Körner, Michal Šimečka, Fabiene Keller, Jan-Christoph Oetjen, Anna Donáth, Maite Pagazaurtundúa, Olivier Chastel, concerning the facial recognition app developed by Clearview AI. 10 June 2020. https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-meps-sophie-t-veld-moritz-korner-michal-simecka_en (last accessed: 11 April 2021)

[51] Council of Europe (2021) Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data. Convention 108: Guidelines on Facial Recognition 28 January 2021 https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3 (last accessed: 21 April 2021)

3.3.1. Semantic modelling

The use of semantic representations and semantic modelling raises few legal concerns directly; however, the use of such technologies can more easily facilitate the linking, combining or matching of datasets which may require an organisation to carry out a DPIA under the GDPR to evaluate the impact of such processing if they related to personal data. Furthermore, semantic reasoning engines or ontologies that support inferencing could lead to profiling or automated decision-making based on the output from such processing. Therefore, as such models are built and incorporated into the system they should be further scrutinised to ensure, as is currently planned, that they do not involve the processing of personal data. This section will be revisited in more detail in D2.6 to ensure this is still the case as the system evolves.

3.3.2. Wearables and health data

7SHIELD foresees the use of wearable IoT sensors to monitor the deployment of tactical decision support teams in the event of a security incident at the ground segment. The use of IoT sensors that measure a first responders' GPS, heart rate, and temperature (e.g.) provide specific health related data relating to that individual. Such data, given that the identity of the individual will likely be known to those monitoring the data constitute special categories of personal data and thus should rely on explicit consent to process such data. Furthermore, such monitoring activities, depending on the context, could constitute systematic monitoring of a person and thus may require the use of a DPIA by the organisation prior to the deployment of such technology on a wider scale. In addition, if decisions are made based on a sensor reading about the individual wearing the sensor, then care must be taken to ensure this is not an automated decision and is taken in context. The capture of health data could also potentially identify a medical issue related to the wearer. A clear policy on how such findings should be managed and communicated may also be necessary.

3.3.3. Social media communications

7SHIELD foresees two potential uses for social media within the system. The first has already been discussed above in the cyber and threat detection and data acquisition section (3.2.1) and notes the legal requirements for complying with data protection and data privacy. The other side of social media is to consider how authorities and operators can use social media to communicate with citizens during an incident. As has already been mentioned in Section 2.3.1 above, recent proposed legislation places a potential duty on authorities to communicate with the public in the event of certain incidents. In addition to the use of traditional media (TV, radio, news), the use of social media is also now a legitimate and rapid means of communicating with many demographics. Therefore, the use of social media may assist authorities in complying with these requirements.

3.3.4. Drone operations

The use of drones (or unmanned aerial vehicles (UAVs) or remotely piloted aircraft system (RPAS)) has increased substantially over recent years. While previously they were utilised mostly in military applications, their use for civil applications has become more common. Furthermore, drones operated by others may also be seen as a security threat to CI sites in the context of 7SHIELD. The agency responsible for drones in the EU is EASA – the European Union Aviation Safety Agency[52] (established through Regulation (EU) 2018/1139)[53] that ensures uniform application of civil aviation rules across the EU. The operation of drones within the EU is governed by two main pieces of legislation.

- Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft.[54]
- Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems.[55]

Recently the EC has introduced the Commission Implementing Regulation (EU) 2020/639 that amends 2019/947 regarding drone operations where visual line of sight cannot be maintained[56], as well as Commission Delegated Regulation (EU) 2020/1058 of 27 April 2020 amending Delegated Regulation (EU) 2019/945 as regards the introduction of two new unmanned aircraft systems classes[57] and Commission Implementing Regulation (EU) 2020/746 of 4 June 2020 amending Implementing Regulation (EU) 2019/947 as regards postponing dates of application of certain measures in the context of the COVID-19 pandemic.[58]

A further regulation manages what is known as the U-space and ensures that drones and other aviation vehicles can co-exist safely in the same airspace. According to EASA the new U-Space regulatory framework should be published in 2021 and, where relevant, it will be discussed in more depth in D2.6.

From these regulations, drone operations are divided into three separate categories.

[52] EASA – European Union Aviation Safety Agency https://www.easa.europa.eu/

[53] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency. Official Journal L212, pages 1-122. 22 August 2018 http://data.europa.eu/eli/reg/2018/1139/oj

[54] Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft. Official Journal L152, pages 45-71. 11 June 2019. http://data.europa.eu/eli/reg_impl/2019/947/oj

[55] Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems. Official Journal L152, pages 1-40. 11 June 2019. http://data.europa.eu/eli/reg_del/2019/945/oj

[56] Commission Implementing Regulation (EU) 2020/639 of 12 May 2020 amending Implementing Regulation (EU) 2019/947 as regards standard scenarios for operations executed in or beyond the visual line of sight. Official Journal 150, pages 1-21. 13 May 2020. https://eur-lex.europa.eu/eli/reg_impl/2020/639/oj

[57] Commission Delegated Regulation (EU) 2020/1058 of 27 April 2020 amending Delegated Regulation (EU) 2019/945 as regards the introduction of two new unmanned aircraft systems classes. Official Journal L132, pages 1- 17. 20 June 2020. https://eur-lex.europa.eu/eli/reg_del/2020/1058/oj

[58] Commission Implementing Regulation (EU) 2020/746 of 4 June 2020 amending Implementing Regulation (EU) 2019/947 as regards postponing dates of application of certain measures in the context of the COVID-19 pandemic. Official Journal L176, pages 13-14. 5 June 2020. https://eur-lex.europa.eu/eli/reg_impl/2020/746/oj

- Open – this category is for low-risk flights and authorisation is not required before embarking on a flight operation.
- Specific – this category requires an authorisation from the national competent authority which involves conducting a safety risk assessment to identify the conditions for safe operation.
- Certified – this category requires certification of the drone and the operator due to the likely high-risk of the operation. The drone pilot should also be appropriately licenced.

A further distinction on terminology is between drone operators and remote pilots. In some cases, these may be the same single individual; however, in larger operations the drone operator may be an organisation that owns the drone while the remote pilot is the person who is flying the drone at a specific point in time. Different legislation and training requirements may apply to the drone operator and the remote pilot.

The regulation 2019/947 became fully operational on the 30 December 2020. The first step for the operation of any drone within the EU is to ensure that operators/pilots are registered with their National Aviation Authority (NAA). The second is to ensure the operator/pilot is educated on the rules, risks and safety considerations for drone operation. The operation of drones in the different categories as specified above have different training requirements.[59] The operator should also verify with the appropriate NAA the insurance requirements to operate the drone, which areas are authorised for flight and if there are any further authorisation requirements necessary to fly the drone.

Open Category

Drones in the open category must either have a classification label of 0, 1, 2, 3, or 4, a privately built drone under 25kg or have no classification label if purchased before January 2023. Drones in the open category must not be flown directly under people unless under 250g or it has a classification label. The remote pilot must retain visual line of sight unless using an observer and should not be flown above 120m. Furthermore, open category drones should not carry dangers goods or drop material. Drones in the open category can be classified in to three subcategories, the weight restrictions, flight restrictions, registration, training and age restrictions of each of these categories are show in the table represented in Figure 2 and produced by EASA[60].

[59] EASA (n.d) Civil drones (Unmanned aircraft). European Union Aviation Safety Agency. https://www.easa.europa.eu/domains/civil-drones-rpas (last accessed: 6 April 2021)

[60] EASA (2021) Requirements under the 'open' category https://www.easa.europa.eu/the-agency/faqs/requirements-under-open-category

<table>
<tr><th colspan="2">UAS</th><th colspan="2">Operation</th><th colspan="3">Drone Operator/pilot</th></tr>
<tr><th>Class</th><th>MTOM</th><th>Subcategory</th><th>Operational restrictions</th><th>Drone Operator registration</th><th>Remote pilot competence</th><th>Remote pilot minimum age</th></tr>
<tr><td>Privately built</td><td rowspan="3">< 250 g</td><td rowspan="3">A1
(can also fly in subcategory A3)</td><td rowspan="2">- may fly over uninvolved people (should be avoided when possible)
- no fly over assemblies of people</td><td rowspan="3">No, unless camera / sensor on board and a drone is not a toy</td><td>- no training needed</td><td>No minimum age</td></tr>
<tr><td>0</td><td rowspan="2">- read user's manual</td><td>16*, no minimum age if drone is a toy</td></tr>
<tr><td>Legacy drones (art. 20)</td><td>16*</td></tr>
<tr><td>1</td><td>< 900 g</td><td>- No expected fly over uninvolved people (if happens, should be reduced)
- no fly over assemblies of people</td><td>Yes</td><td>- read user's manual
- complete online training
- pass online theoretical exam</td><td>16*</td></tr>
<tr><td>2</td><td>< 4 kg</td><td>A2

(can also fly in subcategory A3)</td><td>- no fly over uninvolved people
- keep horizontal distance of 30 m from uninvolved people
(it can be reduced to 5 m if low speed function is activated)</td><td>Yes</td><td>- read user's manual
- complete online training
- pass online theoretical exam
- conduct and declare a self-practical training
- pass a written exam at the CAA (or at recognized entity)</td><td>16*</td></tr>
<tr><td>3</td><td rowspan="4">< 25 kg</td><td rowspan="4">A3</td><td rowspan="4">- fly away from people
- fly outside of urban area (150 m distance)</td><td rowspan="4">Yes</td><td rowspan="4">- read user's manual
- complete online training
- pass online theoretical exam</td><td rowspan="4">16*</td></tr>
<tr><td>4</td></tr>
<tr><td>Privately built</td></tr>
<tr><td>Legacy drones (art. 20)</td></tr>
</table>

Figure 2: Overview of rules and regulations for the operation of drones in the open category

Specific Category

A drone is classified in the specific category if it is not part of the open category[61]. Drones in the specific category must have authorisation from their NAA unless it falls under one of the two standard scenarios listed in Appendix 1 of the implementing regulation 2020/639/EC[56] which are namely:

- operations executed in visual line of sight ('VLOS'), at a maximum height of 120 m over a controlled ground area in a populated environment using a CE class C5 UAS (unmanned aircraft system)
- operations that could be conducted beyond visual line of sight ('BVLOS'), with the unmanned aircraft at a distance of not more than 2 km from the remote pilot with the presence of airspace observers, at a maximum height of 120 m over a controlled ground area in a sparsely populated environment and using a CE class C6 UAS.

[61] EASA (2021) Specific Category - Civil Drones https://www.easa.europa.eu/domains/civil-drones-rpas/specific-category-civil-drones (last accessed: 21 April 2021)

In these cases, a declaration should be made to the NAA but no further action is required provided all relevant training has been completed. If the operation does not fall into one of these categories, then, in most circumstances operators should complete a risk assessment of intended operation or a predefined risk assessment.

Drones in the **certified category**[62] will likely not apply to 7SHIELD operations at this time.

Drone flights within 7SHIELD must obtain all of the required authorisations in order to operate at the piloting sites during test. Specific requirements will be necessary for each test depending on national legislations, some of which are covered in Section 4 below. Furthermore D9.6 will detail of both the safety procedures and flight approvals for each of the piloting activities.

3.3.5. Autonomous operation of drones and drone neutralisation

Drones that operate autonomously fall into the special or certified categories of drone operations. There is a distinction between autonomous and automatic drones which are allowed to operate in all categories and have a pre-determined route to follow. An automatic drone must have a remote pilot available to intervene should an unexpected event occur.[63]

Drones can pose a threat to critical infrastructure either by enabling bad actors to surveil the area to facilitate access to the site or by enabling the deposit of items inside the perimeter of the Ground Segment (such as explosives). Therefore, methods to counter or neutralise drones may be necessary to prevent unauthorised access. To counter drones it is necessary to either target the drone itself, target the person operating the drone or interfere with the communication between the drone pilot and the drone. 7SHIELD focuses on technology that targets the drone directly; however, there is little standardisation at the EU level with no harmonised legislation. This leaves it to the national aviation authorities to determine the legal requirements for counter-drone methods within their national borders.

3.4. Mitigation technologies

In response to mitigation technologies and strategies, at this stage we refer back to the discussion on the legislation related to the protection of critical infrastructure and the NIS Directive with respect to their service and business continuity measures. While not legislative, a recent survey by the European Reference Network for Critical Infrastructure Protection (ERNCIP) considered how well different CI domains were prepared for the impact of the COVID-19 pandemic on their business continuity measures;[64] a particularly

[62] EASA (2021) Certified Category - Civil Drones. https://www.easa.europa.eu/domains/civil-drones-rpas/certified-category-civil-drones (last accessed: 21 April 2021)

[63] EASA (2021) What is the difference between autonomous and automatic drone? https://www.easa.europa.eu/faq/116449 (last accessed: 10 April 2021)

[64] Galbusera, L., Cardarilli, M., & Giannopoulos, G. (2021). The ERNCIP survey on COVID-19: Emergency & Business Continuity for fostering resilience in critical infrastructures. Safety Science, 105161. https://www.sciencedirect.com/science/article/pii/S0925753521000047

clear result highlighted the interdependencies between sectors and the impact that had on their overall response measures.

In relation to recovery from cyber-attacks, the NIS group has published a reference document on security measures for OES which was previously discussed in Section 3.1.2 referencing the measures proposed for secure authentication. Part 4 of the same document[45] also discussed measures related to resilience including provision for the continuity of operations including business continuity measures and disaster recovery management which should be in line with their information system security policy.

Business continuity for critical entities also forms a part of the proposed directive on the resilience of critical entities requiring them to ensure they are able to '*recover from incidents, including business continuity measures*'.

4. National legislation for the pilot use case countries

The developed 7SHIELD system will be piloted in five different use case scenarios each located in a different country (Finland, Spain, Greece, Belgium and Italy). In the scope of this deliverable, it is not possible to assess the applicable legislation in each EU member state (in terms of where it differs from EU law or where specific national legislation applies). Therefore, we perform an initial assessment of what legislation applies in the five piloting countries. To this end, each end user was asked to identify relevant legislation applicable to their use case relating to data protection (which is discussed in Section 6.1), national laws on the protection of national CI, application of the NIS directive, and on the technological aspects (facial recognition, use of drones, use of CCTV). In the below we discuss each of the PUCs in turn along with the legislative considerations. A copy of the questionnaire sent to end users in included in Annex 1. In addition to the response from end users and pilot operators we also made use of the GDPR implementation Toolkit[65] and sites such as DroneRules.eu and the EC's digital single market strategy to cover the implementation of the NIS Directive.

4.1. PUC1 Arctic Space Centre, Finland

The Arctic Space Centre hosts significant technical infrastructure that processes and delivers satellite data. PUC1 focuses on potential physical threat to the GS by unauthorised personnel accessing the site.

National Critical Infrastructure and Ground Segment Protection

In Finland, there are several legislative acts that apply to the protection of national critical infrastructure, these include specific exemptions from the *principle of openness* under the Act on the Openness of Government Activities 621/1999[66]. Other acts that may apply in specific circumstances include those relating to nuclear power, defence, restrictions on the use of land and specific building regulations. Furthermore, in some case legislation relating to the environment or border surveillance activities may apply although these are not within the scope of 7SHIELD.

Cybersecurity

The NIS Directive is transposed into national Finnish legislation[67] and has developed its national strategy on the security of network and information systems.[68]

[65] Practical Law Data Privacy Advisor (n.d.) GDPR National Implementation Legislation Toolkit. Thomson Reuters Practical Law. https://uk.practicallaw.thomsonreuters.com/w-020-2281 (last accessed: 25 April 2021)

[66] Act on the Openness of Government Activities (621/1999 English) [Finland] https://www.finlex.fi/en/laki/kaannokset/1999/en19990621 (English translation)

[67] EC (2019) Implementation of the NIS Directive in Finland https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-finland (last accessed: 21 April 2021)

[68] Ministry of Transport and Communications (2016) Information Security Strategy for Finland The World's Most Trusted Digital Business Environment. https://julkaisut.valtioneuvosto.fi/handle/10024/75353

Video Surveillance and Facial Recognition

Within Finland the Constitution 731/1999[69] protects everyone's privacy and enshrines the right to secrecy of personal communication (letters, phone calls etc). According to the Criminal Code of Finland *(39/1889).*[70] *chapter 24 as amended by law 531/2000*[71], illicit observation is a criminal offence, as is disclosing someone's private information. Finland has a Law on the protection of privacy in working life (759/2004)[72] that restricts camera surveillance in the workplace, which is only permitted for security or monitoring production process. Camera surveillance is not allowed for monitoring certain employees unless they ask for camera surveillance themselves for their own security or rights. The use of such surveillance requires openness and transparency.

Drone operations

In Finland, the main applicable laws for the operation and flying of drones are the 'Aviation act 864/2014',[73] its amendment 534/2020 and the 'OPS M1-32'[74] According to the DroneRules site[75,76] when flying a drone for commercial, scientific or manufacturer testing purposes, above industrial sites and urban areas or beyond line of sight, a drone operator or pilot must registered national and abide by the applicable legislation stated above, have a national identity plate, have an automatic flight control with manual override, have Third Party Liability insurance with a coverage of at least €1millon whilst not impeding any manned aircraft, operate a drone that weighs more than 25kg or fly in a restricted area.

In the case of drone neutralisation, according to Police Act 872/2011[77] as amended by 540/2020[78]. A policeman has the power to shoot a drone down. However, this is not one of the foreseen methods of drone neutralisation within 7SHIELD.

4.2. PUC2 DEIMOS Ground Segment, Spain

PUC2 focus on a cyber-physical attack at the DEIMOS ground segment in Spain with the goal of ensuring secure physical and cyber access.

---

[69] Constitution of Finland, The (731/1999 English) [Finland] https://www.finlex.fi/en/laki/kaannokset/1999/en19990731 (English translation)

[70] Criminal Code of Finland, The (39/1889 English) [Finland] https://www.finlex.fi/en/laki/kaannokset/1889/en18890039 (English translation)

[71] Laki rikoslain muuttamisesta (531/2000) [Finland] https://www.finlex.fi/fi/laki/alkup/2000/20000531 [EN: Law amending the Criminal Code]

[72] Act on the Protection of Privacy in Working Life (759/2004 English) [Finland] https://www.finlex.fi/en/laki/kaannokset/2004/en20040759 (English translation)

[73] Aviation Act (864/2014 English) [Finland] https://www.finlex.fi/en/laki/kaannokset/2014/en20140864 (English translation)

[74] OPS M1-32 (TRAFICOM / 42450 / 03.04.00.00 / 2020) Ilmailu: Kauko-ohjatun ilma-aluksen ja lennokin käyttäminen ilmailuun [translation: Aviation: The use of a remote-controlled aircraft and airplane for aviation] https://www.finlex.fi/fi/viranomaiset/normi/498001/46493

[75] DroneRules (2021) Regulations: Finland (FI) https://dronerules.eu/en/professional/regulations/finland (last accessed: 21 April 2021)

[76] DroneRules (2021) National Regulatory Profile – Finland https://dronerules.eu/assets/regulationspdfdownloads/NatinalRegulatoryProfile_Finland.pdf (last accessed: 21 April 2021)

[77] Police Act (872/2011 English) [Finland] https://www.finlex.fi/en/laki/kaannokset/2011/20110872 (English translation)

[78] Laki poliisilain muuttamisesta (540/2020) [Finland]https://finlex.fi/fi/laki/alkup/2020/20200540 (EN: Law amending the Police Act)

National Critical Infrastructure and Ground Segment Protection

In Spanish Law for national CI, the main applicable legislation is Law 8/2011 of April 28 for the Protection of National Critical Infrastructures[79] which aligns Spanish law with Directive 2008/114/EC and provides a standard for the protection of national critical infrastructure. This law is then implemented through the Royal Decree 704/2011 of December 15 which establish The Regulation on the Critical Infrastructures in the development and implementation of Law 8/2011[80].

Apart from the Radio Frequency Allocation for Satellite, which is not directly relevant to 7SHIELD's scope at this point, there is no specific legal framework relating to the operation of GS in Spanish law.

Cybersecurity

In Spanish Law the NIS Directive has been fully transposed into national law with no deviations from the original text. There are two further relevant pieces of cyber security legislation in Spain, the first is the Royal Decree Law 12/2018 of September 7 on The Security of Networks and Information Systems[81] which transposes the NIS Directive into Spanish Law and the second is the Royal Decree 43/2021[82] of January 26, developing and implementing Royal Decree Law 12/2018.

Video Surveillance and facial recognition

In Spanish Law the Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights, establishes in its Articles 22 and 89 the regulation on video surveillance systems. This legislation, in part, implements the GDPR into Spanish law as well as providing a legal framework to guarantee citizens digital rights beyond that of the GDPR. Furthermore, the Spanish Data Protection Agency (AEPD) has issued a Guide on the use of video cameras for security and other purposes[83].

In terms of processing of data related to facial recognition, the AEPD has issued notes analysing the use of this personal data[84,85], but there is no specific law in this regard beyond complying what is already directly addressed through the GDPR.

---

[79] Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630

[80] Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. https://www.boe.es/buscar/act.php?id=BOE-A-2011-8849

[81] Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información https://www.boe.es/buscar/doc.php?id=BOE-A-2018-12257

[82] Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-1192

[83] AEPD (2021) Guía sobre el uso de videocámaras para seguridad y otras finalidades. https://www.aepd.es/sites/default/files/2019-12/guia-videovigilancia.pdf

[84] AEPD (2019) Informe 010308/2019 del Gabinete Jurídico de la AEPD sobre la licitud de incorporar sistemas de reconocimiento facial en los servicios de videovigilancia proporcionados por empresas seguridad privada. https://www.aepd.es/es/documento/2019-0031.pdf

[85] AEPD (2020) Informe 0036/2020 del Gabinete Jurídico de la AEPD sobre la utilización del reconocimiento facial para realizar exámenes. https://www.aepd.es/es/documento/2020-0036.pdf

Drone operations

In Spanish law, the Royal Decree 1036/2017, of December 15, which regulates the civil use of remotely piloted aircraft, and amends Royal Decree 552/2014, of June 27, which develops the Air Regulations and common operating provisions for air navigation services and procedures and Royal Decree 57/2002, of January 18, which approves the Air Traffic Regulations[86] is the current legislation related to the operation of drones and remotely piloted aircraft. The DroneRules project[87] notes the following requirements for the operation of drones for commercial purposes. Pilots /operators must:

- register nationally and abide by their national regulations,
- obtain a type Certificate and a Certificate of Airworthiness for drones greater than 25kg,
- obtain a national drone pilot certificate,
- have Third Party Liability insurance with a coverage of €1million, or
- file a NOTAM (notice to airmen).

While they must not

- operate at night-time,
- operate in clouds, above crowds, industrial sites, urban areas and other restricted areas, or
- Fly 400 ft above ground level.

Comprehensive details regulations can be obtained through the DroneRules site.[88]

Furthermore, the AEPD has also issued a specific guide regarding privacy in the use of drones[89] that should also be considered.

Health and biometric data

Finally, regarding the processing of health and biometric data, Article 9 of the Organic Law 3/2018, of December 5, on Personal Data Protection and guarantee of Digital Rights[90], regulates the special categories of data as per the GDPR. Article 90 of the aforementioned law regulates the right to privacy in the use of geolocation systems in the workplace.

[86] Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea. https://www.boe.es/buscar/doc.php?id=BOE-A-2017-15721

[87] DroneRules (2020) Regulations: Spain (ES) https://dronerules.eu/en/professional/regulations/spain

[88] DroneRules (2021) National Regulatory Profile – Spain. https://dronerules.eu/assets/regulationspdfdownloads/NatinalRegulatoryProfile_Spain.pdf

[89] AEPD (n.d.) Drones and Data Protection. https://www.aepd.es/sites/default/files/2019-12/guia-drones-en.pdf

[90] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

4.3. PUC3 National Observatory of Athens Ground Segment, Greece

PUC3 is centred around a combined cyber-physical attack on the ground segment based at the National Observatory of Athens.[91] On the physical side, the GS captures data from eight different satellites while NOA also operates several Copernicus Sentinels Data Hubs[92], some of which have restricted access. Due to the location of the GS it can be prone to the impact of natural disasters and extreme weather conditions while the strategic important of the Copernicus hubs mean they must be resistant to cyber-attacks.

National Critical Infrastructure and Ground Segment Protection

In Greece, the Directive 2008/114/EC of 8 December 2008 "on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection" has been implemented in Greece through Presidential Decree (PD) 39/2011. This is the only horizontal legislative text dealing with the protection of critical infrastructures in the national law, focusing on the threat of terrorism and covering mainly the Transport and Energy sector. The main elements of this legislation consist of the following:

- identifying potential ECIs which both satisfy the cross-cutting and sectoral criteria and shall inform the other Member States which may be significantly affected by a potential ECI about its identity and the reasons for designating it as a potential ECI.
- assessing whether each designated ECI located on its territory possesses an Operator Security Plan (OSP) or has in place equivalent measures. The OSP procedure shall identify the critical infrastructure assets of the ECI and which security solutions exist or are being implemented for their protection.
- assessing whether each designated ECI located on its territory possesses SLO or equivalent. The SLO shall function as the point of contact for security related issues between the owner/operator of the ECI and the relevant Member State authority.
- conducting a threat assessment in relation to ECI subsectors within one year following the designation of critical infrastructure on its territory as an ECI within those subsectors.

Other Ministerial Decisions regulate specific issues related to CIs such as the safety of CI, energy supply security or SEVESO facilities.

Given the Hellenic Police's (HP) role in 7SHIELD their function is also relevant. The HP have the responsibility to protect vulnerable targets within the Greek territory. This can be achieved with two protective measures: safeguarding and surveillance. Vulnerable targets are buildings and installations which, by reason of their destination or persons working or residing there, are likely to be the target of a criminal act.

[91] https://groundsegment.space.noa.gr/
[92] https://sentinels.space.noa.gr/

Criteria for determining the type of protective care of vulnerable targets shall be: a) the status of the target, b) the degree of risk, c) the country of origin, in the case of a foreign target, d) existing information, e) prevailing international and internal crises and events, and f) interstate relations.

Safeguarding is the permanent allocation of police armed personnel in order to deny any possible threat/risk upon its duties.

The other measure is surveillance, which consists of the passage, at frequent intervals, of police officers assigned to that purpose, from targets of premises, to the identification of suspected persons or objects to them, in order to prevent any illegal action to the detriment of those objectives.

Cybersecurity

NIS Directive was fully transposed in Greece through Law 4577/2018 (Government Gazette No A' 199/2018-12-03) and was supplemented by Ministerial Decision 1027/2019 "Issues of implementation and procedures of law 4577/2018" (Government Gazette No B' 3739/2019-10-08), defining the general terms and obligations of Basic Service Operators and Digital Service Providers, focusing on the security incident notification process, the National Cyber Security Authority control procedure, the enforcement procedure, sanctions and the criteria for measuring them, as well as the methodology for determining Basic Service Operators.

In addition, Law 4635/2019 establishes a new General Directorate of Cybersecurity, upgrading the former Directorate of Cybersecurity. The same law provided for the immediate staffing of the General Directorate of Cybersecurity.

The General Directorate of Cybersecurity (General Secretariat of Telecommunications and Post – Ministry of Digital Governance) is the single point of contact for the NIS Directive, the National competent authority for DSPs (Digital Service Providers) and the national competent authority for OES (Operators of Essential Services). The Hellenic Computer Security Incident Response Team (CSIRT) for the NIS Directive is under the Ministry of National Defense (MOD) – Hellenic National Defense General Staff and its mission is to reduce the Nation's risk of systemic cybersecurity and communications challenges.

The General Directorate of Cybersecurity draws up the National Cybersecurity Strategy, which sets out strategic objectives, priorities and policy and regulatory measures to ensure security and IT at national level. The latest Greek National Cyber Security Strategy was approved on 07/12/2020.

Video Surveillance

Within Greek Law 4624/2019 on article 27 par. 7 foresees the following:

"The processing of personal data through a closed-circuit optical recording system in workplaces, whether publicly accessible or not, is permitted only if it is necessary for the

protection of persons and goods. Data collected through a closed-circuit optical recording may not be used as a criterion for the evaluation of employees' efficiency. Employees are informed in writing either in printed or in electronic form for the closed-circuit optical recording's installation and operation in the workplace."

In the same context, Article 14(5) of Law 3917/2011, permits the installation and operation of surveillance systems by public authorities, natural or legal persons in the premises they manage, for the purpose of protecting persons and goods, in accordance with the provisions of Law 2472/1997 (as replaced by 4624/2019) and the guidelines issued by the Hellenic Data Protection Authority (HDPA).

According to article 14 par.2 of Law 3917/2011, image recording in public places for the purposes of crime detection and prevention is permitted only by State authorities and when in compliance with the principle of proportionality. As stated in par. 4 of the same article, retention periods as well as the appropriate technical and organizational measures regarding data process will be further specified ad hoc and by presidential decree.

This legislation is supplemented by Directive 1/2011 issued by the HDPA. The Directive concerns the processing of image and/or audio data carried out through video surveillance systems by all public bodies or by natural or legal persons for the purpose of protecting persons and/or goods including specific cases of the provision of health services. In particular, Article 2(a) of the Directive defines the scope and purposes of the processing as follows: *The purpose of the protection of persons and/or goods is justified by the legitimate interest or legal obligation of the owner or manager of an area to protect the site and the goods found in that area from illegal acts. The same applies to the safety of life, physical integrity, health and property of third parties legally located in the supervised area.* For example, the protection of installations and critical infrastructures (e.g., electromechanical equipment for infrastructure networks). The protection of persons and/or goods with video surveillance systems may be sought either by the relevant public or municipal authority or legal person governed by public law who manages or has in accordance with the applicable legislation relevant competence in a particular area or by a legal person governed by private law or a natural person who manages the site or has a legal right or obligation under the provisions of law or in the performance of a contract with the owner of the site.

Article 4 of the directive defines systems which are permanently installed in a space, operating continuously or at regular intervals and capable of receiving and/or transmitting an image and/or audio signal from that space to a limited number of projection screens and/or recording machines (2/2010 Opinion of the Authority, paragraph 8). The image may be transmitted by direct connection of the camera to the projection screen and/or to the recording machine or via an internal network or over the internet for a limited number of eligible recipients. In accordance with Article 7 and the application of the principle of proportionality, it is of particular importance in the case of the operation of video surveillance systems in workplaces. The system should not be used for the surveillance of

workers within such premises, except in specific exceptional cases where this is justified by nature and working conditions and is necessary to protect the health and safety of workers or to protect critical infrastructures (e.g., military factories, banks, high-risk installations). For example, in a typical business office space, video surveillance should be limited to entry and exit areas, without supervised specific office rooms or corridors. Exception may be specific areas, such as cashiers or spaces with safes, electromechanical equipment, etc., provided that the cameras focus on the good they protect and not on the premises of the workers. Also, in special areas, such as areas with electromechanical installations, the shift manager or the safety officer may monitor the operators of high-risk machinery in real time, in order to intervene immediately if a safety incident occurs. In any event, data collected through a video surveillance system may not be used as exclusive criteria for assessing the behaviour and efficiency of employees (see Directive No 115/2001 on the processing of employees' personal data, Section E, par. 6 – 8). The Directive then defines the time of retention, the transfer of data to third parties, the obligation to disclose, the confidentiality and security of processing, and the obligation to inform. More specifically, according to article 8 (par.1) of the Directive, data (including images) must be held for specific time period which is related to every specific purpose of the processing. In any case, provided that no incident related to the purpose of image processing occurs, data must be destroyed at the latest time period of fifteen days and without prejudice to more specific provisions. In case of an incident (e.g., robbery, burglary, etc) against a person or a data controller, images that have recorded can be kept in a separate file for 30 days (par.2). Finally, in case of an incident related to a third person, data controller is permitted to keep the recorded images for 3 months.

Additionally, by authorization of Law 3917/2011 (art.14, par.4), the Presidential Decree (PD) 75/2020 was issued, in order to define the legislative framework related to the use of video surveillance systems (sound or video reception), in public places, to the extent that personal data is processed, in order to effectively achieve the purposes provided in Article 14 of Law 3917/2011, while ensuring the rights of persons affected by the use of these systems.

The installation and operation of surveillance systems by the reception or recording of sound or video in public places is permitted, in accordance with Article 14 of Law 3917/2011, for the following purposes: a) The prevention and suppression of specific criminal acts, such as violent crimes, drug trafficking, etc., and b) traffic management, the regulation of vehicle traffic, as well as the prevention and management of road accidents (article 14 par. 1 Law 3917/2011 and article 3 PD 75/2020).

Public spaces are considered a) those intended for common use according to the standing legislation and city plans, b) freely accessible open spaces to an indefinite number of persons, fenced or not, which are made available for common use in a lawful manner, and c) public transport passenger traffic stations.

In case another public authority (not a Law Enforcement Authority) uses or needs to use the surveillance system, a responsible is nominated for processing and the provisions of articles 26 of the EU Directive 2016/680 for Joint Controllers and article 61 of the National law 4624/2019 are applied.

Conditions and criteria for installation and operation of surveillance systems are referred in Article 5 of the PD 75/2020.

Facial recognition

The Data Retention EU Directive (2006/24/EC)[93], was incorporated into national legislation with the law 3917/2011. Article 14 describes the rules about video surveillance systems in public places. By authorisation of law 3917/2011 (art.14, par.4), Presidential Decree (PD) 75/2020 was issued, in order to analyse issues related to the use of video surveillance systems. Article 2 of the aforementioned PD specifies the surveillance systems, while according to the opinion No. 3/2020 of the *HDPA*, the image of a person, which is collected with a camera, is considered personal data as it is possible to identify the specific person directly or indirectly, while the recording of the image, which is stored and maintained in a device such as a hard disk, constitutes data processing. In addition, it is pointed out that any installation and use of additional equipment, including software for further processing of image and sound, may involve different, independent and distinct processing, in relation to the initial act, storage and preservation, such as in case of "facial recognition software" or possibly in case of "artificial intelligence". So, in the case of using face recognition software, the procedure for the protection of personal data should be independently followed, regardless the fact that the systems used for surveillance are legal. The specific procedure, required to be followed, depends on the use of the equipment, as provided for the national legal framework by Law 4624/2019, as well as GDPR (EU) 2016/679.

According to article 44 of Greek Law 4624/2019 par.1 lit.12, "biometric data" are personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person. Facial recognition technologies are regulated under the term "biometric data" and the term "special categories" in general. The general rule is that the processing of these data is forbidden, except for specific explicit circumstances, which are regulated under the Articles 22 "Processing of special categories of data" (implementing GDPR) and 46 "Processing of special categories of data" (art.10 of Directive) of the national law.

In addition, the following decision of the HDPA No3/2020 "any installation and use additional equipment which incorporates software intended for "Further processing of

[93] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0024

image and sound" may refer to a different, independent and distinct processing in relation to the original collection, storage and preservation of material, such as e.g., in case of using identification software and facial recognition or, where appropriate use of AI. In that case should be followed all processing and legal principles, as well as requirements compliance with the obligations arising from the provisions of Articles 7, 8, 52 par. 1 Charter of Fundamental Rights of the European Union and Article 8 ECHR. This is in consistency with the recent announcement made by the European Data Protection Board (EDPB), which states that the use of some AI services for law enforcement purposes may be inconsistent with the institutional framework of the EU to protect against processing personal data.[50]

Drone operations

In Greece, there are a number of regulations pertaining to the operation of drones, these include the aforementioned EU regulations 2019/945, 2019/947 which have been amended by 2020/1058 and 2020/746 respectively, as well as 2020/639.

Regulation 2019/947 as amended, has entered into force on 1/1/2021 in all Member States; it is therefore applicable in Greece as well. Before the entry into force of Regulations 2019/945 and Regulation 2019/947, Greek Ministerial Decision No Δ/**ΥΠΑ**/21860/1422 (Government Gazette No B' 3152 30.09.2016) issued by the Commander of Civil Aviation Service consists the "Regulation – general framework for Unmanned Aircraft Systems – UAS" is applicable. Its purpose was the setting out of terms and conditions of drones' operation. Furthermore, it explains the air traffic for conducting drone flights. Finally, it explains the risk identification and avoidance of conflict in the "Specific" and "Certified" Category. Competent authority for the drone flights in Greece is the Hellenic Civil Aviation Authority (HCAA). Within the same context, Greek Ministerial Decision No **ΥΠΑ**/Δ2/Δ/30005/12541/2016 Government Gazette No B' 4527-30.12.2016, sets the terms and conditions of Training Centers and licensing of drone users. Information can be found in the official website of the HCAA[94].

In relation to the material collected by drone cameras and its use, Law 4624/2019 about personal data is applicable, as well as:

- L. 2225/1994 about the protection of freedom of correspondence and communication, as modified by L. 4531/2018.
- L. 3115/2003 about the protection of privacy of communications.
- Presidential Decree No 47/2005 about the procedures as well as technical and organizational warranties of the removal of privacy of communications and its protection.

[94] Ministry for Infrastructure and Transport Hellenic Civil Aviation Authority - Authorization Request for UAS (drone) flights http://www.ypa.gr/en/HCAA_UAS_FLT_request_editable.pdf

- L. 3917/2011 about the retention of data produced or processed in connection with the provision of publicly available electronic communications services or public communications networks, the use of surveillance systems when receiving or recording audio or video in public places and related arrangements.

Health and biometric data

The article 23 of the National Law 4624/2019 based on paragraph 4 of Article 9 of the EU GDPR, introduces an additional restriction on Genetic Data Processing according to which the processing of genetic data for health and life insurance purposes is prohibited.

4.4. PUC4 ICE Cubes Service

The ICE Cubes service, operated in a collaboration between SPACEAPPS and ESA, allows private entities to conduct experiments on the International Space Station. Given the sensitivity of the asset, continuous cyber threat detection is essential.

National Critical Infrastructure and Ground Segment Protection

The Critical Infrastructures Act[95] implements the Directive 2008/114/EC, which, as discussed above, focuses on the energy and transport sectors.

Cybersecurity

The NIS Directive is fully transposed into Belgian Law[96] and their national strategy on the security of network and information systems has been made available from the Centre for Cyber Security Belgium[97].

Video surveillance and facial recognition

The Belgian DPA does explicitly consider aspects relating to video surveillance or CCTV; however, processing of video data is subject to the Belgian DPA except in specific circumstances. There is legislation that limits the use and installation of video surveillance in public spaces based on the 2007 Act[98] and the updated 2018 Act.[99] Furthermore, the Royal Decrees on the installation, use, and registration of surveillance cameras[100] and on

[95] Law of 1 July 2011 on the security and protection of critical infrastructures (updated 25/09/2018) // Loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques (mise à jour au 25/09/2018) http://www.ejustice.just.fgov.be/eli/loi/2011/07/01/2011000399/justel

[96] EC (2019) Implementation of the NIS Directive in Belgium https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-belgium (last accessed: 21 April 2021)

[97] Centre for Cyber Security Belgium (2012) National Cyber Security Strategy https://ccb.belgium.be/en/organisation

[98] Act of 21 March 2007 governing the installation and the use of surveillance cameras (English translation) https://journals.sas.ac.uk/deeslr/article/view/2312/2263

[99] Law of 21 March 2007 regulating the installation and use of surveillance cameras // Loi 21 Mars 2007 réglant l'installation et l'utilisation de caméras de surveillance http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2007032139&table_name=loi

[100] Royal Decree relating to declarations of installation and use of surveillance cameras and the register of surveillance camera image processing activities (amended by RD of 02/12/2018) // Arrêté royal relatif aux déclarations d'installation et d'utilisation de caméras de surveillance et au registre d'activités de traitement d'images de caméras de surveillance (8 Mai 2018) http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2018050818&table_name=loi

establishing how camera surveillance takes place all apply in cases of video surveillance.[101] Workers' rights are also protected in terms of the use of video surveillance cameras in the workplace.[102]

Drone operations

According to the DroneRules profile,[103] within Belgium the Royal Decree RPAS 10 April 2016 applies to the professional use of drones. Drone operators and pilots must abide by this legislation and

- register nationally and have an identity plate, a drone identification number visible on fuselage and a Drone Pilot Certificate,
- pass a theoretical and practical exam,
- have Third Party Liability insurance with a coverage of €1 million, and
- always respect privacy and data protection laws.

While drone pilots must not fly in restricted areas or populated areas without authorisations, have a fully manual or automatic flight control system or fly at an altitude of more than 90 meters[104]. Further, the Belgian Mobility and Transport site provides specific information for drone operators to ensure they are in line with all national legislation.[105]

Health and biometric data

Belgian implements some restrictions through the GDPR on the processing of special categories of personal data. These are discussed further in Section 6.1.

4.5. PUC5 ONDA DIAS Platform

PUC5 is run by Serco Italia using their ONDA platform, which is one of the European Space Agency's (ESA) five Data and Information Access Services (DIAS). ONDA supports open access to data from the Sentinel satellites as well as other Earth Observation missions and other projects from Copernicus. Therefore, many people and organisations rely on access to the ONDA services every day. PUC5 concerns the impact on the ONDA services if it were to come under a cyber-attack, namely a denial-of-service attack rendering the service inaccessible to many of its users. Although PUC5's focus is on a cyberattack, given it is

[101] Royal decree defining how to report the existence of camera surveillance // Arrêté royal définissant la manière de signaler l'existence d'une surveillance par caméra (modifié par les arrêté royaux des 21 août 2009, 28 mai 2018, 2 décembre 2018 et 23 mars 2020) http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2008021041&table_name=loi

[102] Convention collective de travail n° 68 conclue le 16 juin 1998 au sein du Conseil national du Travail, relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu du travail. - Enregistrée le 13 juillet 1998 sous le n° 48678/CO/300. http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1998061645&table_name=loi

[103] DroneRules (2021) National Regulatory Profile – Belgium https://dronerules.eu/assets/regulationspdfdownloads/NRP_belgium.pdf

[104] DroneRules (2021) Regulations: Belgium (BE) https://dronerules.eu/en/professional/regulations/belgium

[105] https://mobilit.belgium.be/fr/transport_aerien/drones

operated out of a physical ground segment we address the legal landscape for the deployment of the 7SHIELD system as a whole.

National Critical Infrastructure and Ground Segment Protection

In 2016, Italy launched its Space Economy Strategic Plan[106] whereby the Space Economy is considered as *the value chain that, starting from the research, development and manufacture of enabling space infrastructures, (the so-called "Upstream"), goes up to the manufacture of "enabled" innovative products and services, (the so-called "Downstream: environmental monitoring and weather forecast services, etc.). The growth of the Downstream will be mainly due to the spread of a significant quantity and variety of added value services with a strong territorial connotation.*

The goal for the national space sector is to become an engine of growth within Italy. Developed around scientific and technical excellence, the aim is to extend the impact and benefits to the whole industrial and production system, thus delivering sustainability.

The ASI (Agenzia Spaziale Italiana), within the framework of its statutory mandate, provides its technical-operating contribution to the development of Space Economy programmes and activities that can be implemented also to investments outside the budget of the Agency.

Its purpose is to allow Italy to change the national space sector, that employs about 6,000 people in Italy and is an asset worth 1.6. billion euros in annual revenue. The development of the national space sector is strongly influenced by the availability and allocation of public resources to support the national programmes, European commitments and the competitiveness of the industry chain.

Cybersecurity

Within 7SHIELD, both the NIS Directive and the Cybersecurity Act both apply with Italy. At this stage the NIS directive has been fully transposed into Italian law[107] and the national strategy on the security of network and information systems is available.[108]

Video surveillance and facial recognition

In Italy the "Video Surveillance ' Decision dated 8 April 2010"[109] sets out the obligations for the deployment of CCTV and other video surveillance mechanisms.

In the case of processing data obtained through video surveillance it must be grounded in any of the lawfulness preconditions expressly referred to in the data protection code for

[106] Agenzia per la Coesione Territoriale – Space Economy Strategic Plan. https://www.agenziacoesione.gov.it/s3-smart-specialisation-strategy/piano-strategico-space-economy/?lang=en

[107] EC (2019) Implementation of the NIS Directive in Italy https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-italy

[108] Presidenza del Consiglio dei Ministri (2017) Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf

[109] GPDP (2010) Video Surveillance ' Decision dated 8 April 2010 [1734653] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1734653

public bodies. These conditions include the discharge of institutional functions, and for private or for-profit entities this must also include the fulfilment of legal obligations and the compliance with a so-called "balancing of interest" decision, alongside free and explicit consent by the data subject.

These preconditions are applicable to different sectors, in the public sector every IT system including the respective software to be designed from the start in such a way as to not use data related to identifiable individuals if the purposes of the processing can be achieved by only relying on anonymous data – e.g., by configuring the software to only enable bird´s-eye views in monitoring road traffic without zooming in images and making individuals identifiable. This is a requirement arising out of the data minimization principle, whereby IT systems and software should be configured in order to minimize the use of personal data.

In the private sector, for video surveillance to be carried out in compliance with the proportionality principle when selecting filming arrangements and location (e.g. the use of fixed or pan-tilt cameras with or without zooming) as well as in the course of the processing of data, which must be in any case relevant and not excessive in connection with the purposes to be achieved.

Drone operations

ENAC is the Italian Civil Aviation Authority that sets out the requirements for the operation of drones.[110,111] These requirements include:[112]

- Drones and the remote pilot ground station must have a plate showing the identification of the system and of the operator. If data is to be transmitted electronically in real-time, they must be equipped with an Electronic Identification Device.
- Drone pilots must maintain a direct line of sight.
- Drones cannot be flown at night-time.
- Drones must operate at least 50m away from people and 150m away from congested urban areas.
- Drones cannot fly over people or crowds.
- Drones flown for commercial purposes may not fly more than 150 above ground.
- Drones may not be flown within 5km of any airport or airfield.

Furthermore, commercial drone pilots conducting low-risk operations must submit a statement of compliance with specific requirements to ENAC along with a fee. For higher-

[110] ENAC (2016) Regulation: Remotely Piloted Aerial Vehicles (English translation) https://dronerules.eu/assets/covers/National-Regulation_ITALIA_EN.pdf (last accessed: 22 April 2021)
[111] DroneRules (2021) Regulations: Italy (IT) https://dronerules.eu/en/professional/regulations/italy (last accessed: 22 April 2021)
[112] UAVCoach (2020) Drone Laws in Italy https://uavcoach.com/drone-laws-in-italy/ (last accessed: 22 April 2021)

risk operations commercial drone pilots must obtain training, an operating certificate and a health certificate.

Health and biometric data

In the main the implementation of the GDPR in Italian law did not introduce specific derogations for the processing of health data; however, a later update post-GDPR included further guidance which restricts the sharing of health data with unspecified persons.[113]

[113] Practical Law (n.d.) Italian Implementation of the GDPR. Thompson Reuters Practical Law https://uk.practicallaw.thomsonreuters.com/w-019-8933?documentSection=co_anchor_a920814

5. Ethical and societal framework

Societal acceptance of advanced technologies for security and resilience is essential. Such acceptance can only be achieved if the full range of ethical issues are taken into consideration alongside the legislative materials. Therefore, in this section we consider the main ethical issues that 7SHIELD address in the development of the system. Firstly, we consider ethics in the context of Space systems, followed by specific ethical issues relating to 7SHIELD's technologies and finally any issues that specifically relate to the piloting countries.

5.1. Ethics and societal impact on the space sector

Satellite data provides essential services to EU citizens through the delivery of earth observation, satellite communication and global navigation systems. Such services are crucial to the normal operation of society providing services that many citizens and organisations depend on daily. In times of crisis, this data can also provide vital information needed for disaster response, policing operations and other critical infrastructure services.

5.2. Societal and ethical considerations for 7SHIELD technologies

The ethical use of advanced technologies and the potential impact they can have on society should be an ever-present consideration during the design, development and deployment of such services. As data protection, privacy, and security by design and default become both standard and legally mandated practices the inclusion of ethics by design is also becoming a standard approach.

When discussing embedding ethics and the societal impact of modern technology, the prevailing narrative is focused on the ethical application of AI-based technology. AI has almost unlimited potential to transform the operation of many industries and sectors; however, such application cannot go unchecked. There is already extensive guidance on the ethical use of AI from all sectors. A recognised starting point is the EC's High-level expert group (HLEG) on AI and their ethics guidelines for trustworthy AI promote three fundamental principles:[114]

(1) The use and application of AI must be **lawful**, respecting all applicable laws and regulations

(2) The use and application of AI must be **ethical**, respecting ethical principles and values

(3) The use and application of AI must be **robust**, both from a technical perspective while taking into account its social environment.

[114] High-Level Expert Group on AI (2019) Ethics guidelines for trustworthy AI https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Within these principles a further seven key requirements are specified to be considered trustworthy. These are:

- **Human agency and oversight** – the idea that AI is there to support human activity and that proper human-in-the-loop and similar approaches must be implemented to provide oversight.
- **Technical robustness and safety** – embedding the principles of accuracy, reliability, and reproducibility as well as safety and security with fallback mechanisms in case of errors to prevent unintentional harm.
- **Privacy and data governance** – over and above data protection and privacy characteristics, the inclusion of data governance to manage and review data quality, integrity and access.
- **Transparency** – with regard to data, systems and AI business models including traceability mechanisms and explanations in accordance with stakeholders' expectations. Signposting when interacting with AI.
- **Diversity, non-discrimination and fairness** - removal of unfair bias to prevent negative consequences such as marginalization and the exacerbation of prejudice and discrimination whilst also ensuring AI technology is accessible to all.
- **Societal and environmental well-being** – ensure AI systems benefit all of society, now and in the future, including sustainability and environment impacts as well as the systems' impact on others.
- **Accountability** – systems should be built with accountability, responsibility and accountability and auditability in mind with opportunities for accessible redress where appropriate.

In 7SHIELD, all applications of AI should strive to adhere to these principles, documentation of the steps taken to ensure compatibility must be detailed and should be considered from the outset of development rather than at the conclusion. This applies to both research within 7SHIELD and any further potential deployments or applications of the system after the project. Compliance is not an activity that can be bolted on but must be considered upfront to ensure optimal and long-lasting results and application.

Similarly, the European Commission's White Paper on AI[115] argues that while AI can do good within society, it can also do harm due to the loss of privacy of individuals involved. The paper goes on to recommend that a regulatory framework should be implemented that concentrates on how to minimise the various risks of potential harm. The 7SHIELD project should ensure that any activity that may infringe a person's right to privacy, in the

[115] EC (2020). 'White Paper on Artificial Intelligence. A European approach to excellence and trust'. European Commission.

operational system, is necessary for the purposes of security, and that clear guidelines are in place as to how this data is managed.

5.2.1. Prevention technologies

5.2.1.1. Risk and vulnerability assessments and cascading effects

Risk and vulnerability assessments are crucial for identifying and considering potential internal and external events that could disrupt the operation of CIs and, the case of 7SHIELD, the GS specifically. As with all risk and vulnerability assessment frameworks the quality of the assessment is highly dependent on the inputs. Recent research has highlighted that in assessing the potential impact of the disruption of a CI there has been a lack of emphasis on how this affects areas such as social vulnerability.[116] Therefore, incorporating such aspects as downstream effects of a failure of a GS should form a component of any risk assessment to ensure the societal impact is more widely considered. This is particularly the case for systems such as GS as citizens may have a clearer conceptual understanding of how they may be affected by an interruption to the supply of water or power but not to space infrastructure. A recent report from the UK, highlighted extent to which society interacts with only the GNSS part of space infrastructure every day,[117] whilst another report detailed further cascading societal effects which included the potential for widespread social disruption.[118]

5.2.1.2. Secure authentication

The legal requirements of secure authentication methods used in the protection of critical infrastructures are discussed in Section 3.1.2, however there are also ethical issues to be considered surrounding the risks to personal data being stored within the 7SHIELD systems. 7SHIELD will design and develop secure authentication mechanisms for data access throughout the project, it is important that both compliance with GDPR and addressing potential ethical concerns are factored in from the outset. In their report on Ethics and Data Protection, the EC[119] stated that the 'data protection by design' concept is one of the best ways to address ethical concerns at the design stage, including measures such as the pseudonymisation or anonymisation of personal data.

Alongside ensuring that the system design enhances the security of personal data, consideration should be given to who is able to access this data. The European Union

[116] Garschagen, M., & Sandholz, S. (2018). The role of minimum supply and social vulnerability assessment for governing critical infrastructure failure: current gaps and future agenda. Natural Hazards and Earth System Sciences, 18(4), 1233-1246.
[117] Innovate UK (2017) Economic impact to the UK of a disruption to GNSS. Showcase Report. London Economics https://www.gov.uk/government/publications/the-economic-impact-on-the-uk-of-a-disruption-to-gnss
[118] Pescaroli, G., Green, L.M., Wicks, R., Bhattarai, S. and Turner, S. Cascading effects of global positioning and navigation satellite service failures. UCL IRDR and Mullard Space Science Laboratory Special Report 2019-02, University College London. DOI: 10.14324/000.rp.10076568
[119] European Commission (2018) Ethics and data protection. https://ec.europa.eu/info/sites/info/files/5._h2020_ethics_and_data_protection_0.pdf

Agency for Cybersecurity[120] states that any person who has access to securely stored personal data should have clearly defined and documented responsibilities and be on a need-to-know basis, which is to be regularly reviewed and updated. It is important to limit the access to 7SHIELD systems, particularly those storing personal data, to only those who require it in order to reduce the possibility of a security breach occurring. This review process should extend to the secure authentication system as a whole, with regular checks to ensure privacy of data.

The methods for secure authentication could also raise ethical concerns. For example, the introduction of biometrics as an authentication mechanism could raise both data protection and ethical concerns.

5.2.2. Detection technologies

5.2.2.1. Online data acquisition

Data acquisition through both open-source methods poses several ethical considerations. The legal considerations of online data acquisition are discussed in detail in Section 3.2.1. Open-source methods include gathering data from social media, the surface web and the dark web. A particular concern in this area surrounds the right to privacy of individuals and the need to minimise the level of collateral intrusion (collecting data on persons not directly associated with your search target). Social media presents a particular issue for avoiding collateral intrusion it is almost impossible to eradicate it completely.[121] The ethics of data privacy here go hand in hand with the legal requirements. The GDPR gives individuals a right to be informed about the collection and use of their personal data (Article 14) except in specific circumstances. However, as mentioned in Section 3.2.1.1, 7SHIELD it is difficult to restrict processing of personal data during online collection; however, as soon as it is identified that data is not relevant it should be erased immediately. Furthermore, mechanisms such as data minimisation should be applied to ensure that the minimum amount of personal data is collected as necessary to carry out the task.

Acquiring data from the dark web raises further ethical concerns beyond the collection of personal data. Due to the structure of the dark web, there is the potential for unexpected collection of illegal data while on the platform.[122] Although the data collection activities will aim to mitigate this risk, it raises ethical challenges about the potential impact on viewers of such material and the extent to which it could be distressing or harmful (in the event of violent, criminal, terrorist or child sexual abuse material) and to who this should be reported. The recommendation is to report any clearly identified illegal content through appropriate

[120] ENISA (2021) Risk level assessment - Security measures https://www.enisa.europa.eu/risk-level-tool/help

[121] Omand, D., Bartlett, J., & Miller, C. (2012). Introducing social media intelligence (SOCMINT). *Intelligence and National Security*, *27*(6), 801-823.

[122] Gercke, M. (2021). Ethical and Societal Issues of Automated Dark Web Investigation: Part 4. In Dark Web Investigation (pp. 169-187). Springer, Cham

national channels where possible and restrict crawling depth to prevent web crawling straying too far from initial entry points.

5.2.2.2. Video surveillance

7SHIELD proposes the use of video surveillance technologies as a means of detecting physical intrusions in GS areas and facilities. 7SHIELD intends to incorporate state-of-the-art methodologies for optical video surveillance to recognize human malicious activities, detect and identify faces, classify objects, and extract multimedia concept from various surveillance cameras.

The deployment of video surveillance technology raises privacy and data protection concerns, many of which have been discussed in Section 3.2.2 as well in each for each PUC country in Section 4. Ethical issues in video surveillance concern both the capture of the footage as well as the processing of such footage and whether it is done in real-time.

Ethics concerning video capture include to what extent non-suspicious persons (e.g., GS employees) are captured and who (if anyone) monitors such data and whether that impacts on employee behaviour (e.g., a chilling effect). In terms of detecting persons or objects, entering into such a space using automated algorithms, ethical concerns could be raised if the number of false positives is unduly high – a threshold for such a consideration should be established. Similarly, on the automated classification or alerting of suspicious behaviours, there should be recourse to improve such algorithms where necessary. Finally, the positioning or location of such systems should also be considered. In 7SHIELD, the capture of public citizens (excluding those trespassing or illegally accessing the site should not be provided for via the video surveillance system.

Going beyond, person detection to facial recognition raises further ethical considerations especially in the context of 7SHIELD. The first question to be considered is who are the persons to be identified and how is such a databased established? If such a database of people to be detected can be created and used lawfully, then all other important aspects for AI research can then be considered.

For facial recognition tasks the possibility of bias embedded within the algorithm from the training approach or data, particularly racial and gender biases, are one of the most well-known concerns. For example, Buolamwini and Gebru found that commercial products classifying individuals as either male or female using automated facial analysis algorithms varied in accuracy depending on the colour of the person's skin and their actual gender, with darker-skinned females being the most misclassified group.[123] Due to the potential for these embedded biases, it is essential to address and mitigate against these issues from outset of 7SHIELD when developing video surveillance technologies. The HLEG on AI stated that such bias could be counteracted by putting in place oversight processes to

[123] Buolamwini, J. and Gebru, T., (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In Conference on fairness, accountability and transparency (pp. 77-91). PMLR.

analyse and address the system's purpose, constraints, requirements, and decisions in a clear and transparent manner, removing any identifiable bias at the dataset collection phase where possible.[114]

As mentioned in Section 3.2.3.2, facial recognition can infringe on the right to privacy by individuals, addressed by the Council of Europe[51] guidelines which calls for stricter rules to avoid the significant risks to privacy and data protection posed by the use of facial recognition technologies. The EU Ethics Guidelines for Trustworthy AI (2019) state that human beings should remain free to make life decisions for themselves, which includes the right to private life and privacy.

To mitigate against ethical concerns, 7SHIELD, training data must either publicly available datasets for which good data provenance can be ascertained with regards to collection methods as well as representativeness, or by direct informed consent for persons who may participate in demonstrations acting as trespassers.

5.2.2.3. Other detection methods

7SHIELD will aim to use state-of-the-art technologies and methods for thermal and near-infrared (NIR) image processing to detect potentially malicious activities near the GS, such as the detection of moving objects and people during the night. Due to these imaging techniques being used only to detect the presence of a live human (or animal), and not for identification purposes, there are fewer ethical concerns than with recognition technology. The main consideration regarding thermal and NIR imaging surround the level of automation of the systems. For example, what warnings are produced when such an intruder is identified and what actions are taken based on the alert. Here 7SHIELD benefits from applying human-in-the-loop oversight mechanisms that can verify whether the intruder is a person, animal or object and what decisions should be taken based on that analysis; such a method is considered a responsible use of technology.[124]

7SHIELD also plans to use sensors such as LIDAR as another method of detection of intruders. LIDAR for detection objects is already used extensively in autonomous vehicles, where the impact of not detecting an object is potentially more severe; as the autonomous decisions made upon detection if they are incorrect. Therefore, the main ethical questions are focused on the impact of detecting/not detecting any intruder and/or classifying a human as an animal or drone as a bird, for example, and the impact that has on decision making. Which is, to a certain extent, a data training problem or a consideration for operators in terms of the amount of tolerance that is acceptable. As with all semi-automated systems, too many false alarms can result in a degree of contempt or mistrust in the system,

[124] Grimond, W., and Singh, A., (2020). 'A Force for good? Results from FOI requests on artificial intelligence in the police force'. [online] The RSA. https://www.thersa.org/globalassets/reports/2020/a-force-for-good-police-ai.pdf (last accessed: 31 March 2021)

while missing a single positive event could also similarly damage perception of its effectiveness.

5.2.2.4. Cyber-attack and vulnerability detection

In cyberspace, recent research has argued that the degree to which ethical concern are considered both in terms of academic work and in practice as limited.[125] Amongst others they note concerns that could be particularly relevant to 7SHIELD including practices for how vulnerabilities should be disclosed if they are identified, how research could impact on the functioning of any live system, and whether this could have a long term impact on the commercial viability of any installed system if catastrophic vulnerabilities are found. They also raise similar concerns for policies on incidental findings.

5.2.3. Response technologies

5.2.3.1. Automated reasoning and decision making

In terms of response technologies, frameworks for classifying data and making inferences on that data all have the potential to embed bias within those decision-making processes. Therefore, following similar processes to the application of AI research and applying principles that monitor and manage bias, transparency, and fairness should all feed into the development of the developed models.

5.2.3.2. Wearables and health data

The introduction of wearables and IoT sensors for health monitoring can provide valuable information during the deployment of operations teams. However, a number of ethical concerns can be raised for the deployment of such technology. For example, wearables that detect health data could make apparent medical conditions known to those who would not usually need to disclose such information to or lead to those with access to the data making judgements about the health of the persons wearing the devices. In the case of GPS devices, there may be concerns about further analysis of the data beyond the initial mission tracking or how such data could be used in post-hoc incident analysis. Therefore, strict controls on who can access such data and the scope of use and retention of such data is essential.

5.2.3.3. Social media communications

Social media is a valuable tool for communicating to a wider variety of citizens and stakeholders in the event of a disaster or as a warning to a forthcoming incident. Engaging in such communication can be fraught with risk and in this context can raise some ethical concerns. The first is not limited to social media, it concerns striking the right tone to communicate the urgency of the message without causing mass panic. The second

[125] Macnish, K., & van der Ham, J. (2020). Ethics in cybersecurity research and practice. Technology in Society, 63, 101382.

consideration involves understanding how recipients may respond to receiving messages relating to crisis situations, for example research on university-age students demonstrated different responses based on gender, while a warning message (of an impending tornado) was considered less seriously than an active shooter scenario.[126] This has further implications for how messages are communicated and the expected impacts of such messages. Furthermore, while the usage of social media is still increasing, there are also still many demographics within society that social media communications may not reach. Therefore, in terms of ethics, the implications of primarily focusing on social media could disadvantage other groups in reacting to the incident. Therefore, 7SHIELD must consider the entire media communications strategy including fallback options for reaching or warning other members of society.[127]

5.2.3.4. Drones and drone neutralisation technologies

The ethical use of drones is another area of hot debate. While many of the ethical dilemmas focus on the military domain, their use in civil applications also requires us to address some ethical concerns.[128] The use of drones themselves may often not be the core issue, but their use is associated with the increase in size of the area that can be monitored through the use of sensors attached to the drone. Within 7SHIELD such surveillance will focus on a targeted approach within the defined perimeter of the GS and not monitor the wider public. Further, ethical concerns could also arise in the context of autonomous drone operations, which, if they use AI-based implementations, should have clearly defined constraints and fallback possibilities to switch to pilot-based operations.

In terms of drone neutralisation, concerns many include safety concerns should the drone fall to the ground (however, the technique applied within 7SHIELD should avoid this). There are also potentially liability concerns if legitimate drone activities are taken down and significant damage was caused to the intruder drone.

5.2.4. Mitigation technologies

In terms of mitigation approaches, many of the considerations raise in Section 5.2.1.1 also apply here in also ensuring the wider context is also considered. Ethics may also play a role in when considering the likelihood of different scenarios to occur and the impacts on different sectors and demographics. For example, biases could influence how the understanding of such aspects may have an impact on different communities especially through wider cascading effects that may be apparent. However, if such differences are not

[126] Sheldon, P., & Antony, M. G. (2018). Sharing emergency alerts on a college campus: How gender and technology matter. Southern Communication Journal, 83(3), 167-178.

[127] Park, S., & Avery, E. J. (2018). Effects of media channel, crisis type and demographics on audience intent to follow instructing information during crisis. Journal of contingencies and crisis management, 26(1), 69-78.

[128] Finn, Rachel L., and David Wright. "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications." Computer Law & Security Review 28.2 (2012): 184-194.

considered in advance such communities could experience more severe impacts if such an event does occur[129].

[129] Cardona, O.D., M.K. van Aalst, J. Birkmann, M. Fordham, G. McGregor, R. Perez, R.S. Pulwarty, E.L.F. Schipper, and B.T. Sinh, 2012: Determinants of risk: exposure and vulnerability. In: Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation [Field, C.B., V. Barros, T.F. Stocker, D. Qin, D.J. Dokken, K.L. Ebi, M.D. Mastrandrea, K.J. Mach,
G.-K. Plattner, S.K. Allen, M. Tignor, and P.M. Midgley (eds.)]. A Special Report of Working Groups I and II of the Intergovernmental Panel on Climate Change (IPCC). Cambridge University Press, Cambridge, UK, and New York, NY, USA, pp. 65-108

6. Legal and ethical considerations for 7SHIELD research

In the context of 7SHIELD research, there are several legal and ethical provisions that apply. In the case of legal provision, the most prominent aspect is the application of the GDPR within 7SHIELD's activities. The GDPR sets out specific provisions under Articles 9(2)(j) and Article 89 of the GDPR for the processing of special categories of personal data for research activities; however, in general all the provisions as discussed in Section 2.2 still apply within a research context and so will not be repeated here for brevity. In the framework of the project, there are several deliverables that set out how 7SHIELD will conduct research with legal frameworks and ethically within the project. These requirements include procedures for the recruitment of research participants and managing informed consent. All participants in 7SHIELD research, through either participant in workshops and/or piloting activities will participate only on the basis of informed consent. In terms of the technology development, all partners have to assess whether a DPIA is necessary for carrying out their research activities and how they comply with the principle of data minimisation as well as ensuring consider all ethical implications of technology develop from inception to deployment.

6.1. National data protection laws for pilot countries

While the GDPR applies Europe-wide, it makes provisions for allowing EU MS (and EEA countries) to introduce specific legislation that enables them to specify, restrict or expand the scope of certain aspects of the GDPR. In this section we have consulted each of the piloting countries (Belgium, Finland, Greece, Italy and Spain) about the particular derogations foreseen within their national legislation under the GDPR mainly focused on any derogations associated with the processing of special categories of personal data under Article 9(2)(j) and Article 89. This has been carried out in conjunction with the GDPR National Implementation Legislation Toolkit[130] to provide additional documentation for each MS.

An area where there is scope in national legislation for further inclusions, that is relevant to the implementation of the pilot cases, is Article 9(2)(j) which relates to the processing of special categories on personal data within a research context (namely archiving in the public interest, scientific or historical research, or statistical purposes). MS can make use of the opening clauses within this Article in order to make adjustments specific to their national requirements. In particular, it is the clauses within Article 15 (access rights), 16 (rectification rights), 18 (restrictions on processing) and 21 (right to object) where specific derogations can apply.

[130] Practical Law - GDPR National Implementation Legislation Toolkit https://uk.practicallaw.thomsonreuters.com/w-020-2281 (last accessed: 22 April 2021)

Belgium

Due to the introduction of the GDPR, Belgium introduced two new pieces of legislation, the Data Protection Authority Act 2017 and the Data Protection Act 2018[131]. In the processing of special categories of personal data, data controllers and public organisations must maintain a list of persons having access to the data and a description of their role in data processing as well as ensuring they are aware of the responsibility to keep the data confidential. According to Article 186 of the Belgian Data Protection Act, in the case of Article 9(2)(j) a number of limitations on data subjects rights' apply when processing data for scientific or historical research or statistical purposes if 'honouring these rights renders impossible or seriously impairs achieving the processing's purpose and restricting the right is necessary to achieve the purposes'[131] (Access rights [A15], Rectification rights [A16], Processing restrictions rights [A16], and Objection rights [A21]). Nonetheless, controllers must inform data subjects whether their personal data will be anonymised and the reason why such rights cannot be maintained.

Finland

Finland introduced the Data Protection Act (1050/2018) as it aligned its national legislation to the GDPR.[132] According to this note on the Finnish Implementation of the GDPR[133] and the English translation of Data Protection Act some derogations apply when processing data for scientific or historical research purposes. These include some derogations from Articles 15 (access rights), 16 (rectification rights), 18 (restriction of processing) and 21 (objection) only if the following apply.

- the processing is based on an appropriate research plan;
- there is a designated person or group is responsible for the research;
- the controller only uses and discloses the data for scientific or historical research purposes or another compatible purpose; and
- the controller does not disclose personal data related to a specific individual to third parties.

If the above derogations are applicable but personal data to be processed includes special categories of personal data then a DPIA must be conducted.

Greece

In Greece, the introduction of the GDPR led to the enactment of law 4624/2019 on the Protection of Individuals regarding processing of personal data.[134] In this legislation, Article

[131] Practical Law - Belgian Implementation of the GDPR https://uk.practicallaw.thomsonreuters.com/w-026-5910 (last accessed: 22 April 2021)
[132] Data Protection Act (2050/2018 English) [Finland] https://www.finlex.fi/en/laki/kaannokset/2018/en20181050
[133] Practical Law – Finnish Implementation of the GDPR. Thompson Reuters Practical Law https://uk.practicallaw.thomsonreuters.com/w-025-3800 (last accessed: 22 April 2021)
[134] Practical Law – Greek Implementation of the GDPR. Thompson Reuters Practical Law https://uk.practicallaw.thomsonreuters.com/w-026-6627 (last accessed: 22 April 2021)

30 introduces an exception from Article 9(1) of the EU GDPR, for the processing of specific categories of personal data which shall be permitted without the consent of the subject when the processing is necessary for scientific or historical research purposes or the collection and maintenance of statistical data when the interest of the controller outweighs the interests of the subject not to have his personal data processed. The controller is obliged to take appropriate and specific measures to protect the legal interests of the data subject. These measures include:

(a) access restrictions for controllers and processors;
(b) pseudonymization of personal data;
(c) encryption of personal data;
(d) definition of DPO.

In further derogations from Articles 15, 16, 18 and 21 of the EU GDPR, the rights of the data subject shall be restricted if their exercise is likely to make it impossible or seriously impede to fulfil the purposes of 9(1) and if the restrictions, they are deemed necessary for their fulfilment. For the same reason, the right of access of the subject provided for in Article 15 of the EU GDPR does not apply, when the personal data are necessary for scientific purposes and the provision of information requires a disproportionate effort.

Except the specific measures which are referred previously, specific categories of personal data when processed for the purposes of the article shall be anonymised as soon as scientific or statistical purposes so permit, unless this is contrary to their legitimate interest of data subject. Until then, attributes that can be used to assign individual details about a personal or factual identity to an identifiable person must be stored separately. These characteristics can be combined with individual details, only if the research or statistical purpose so requires.

In addition, the controller may publish personal data processed in the course of the research, provided that the data subjects have given their written consent or that publication is necessary for the presentation of the results of the research. In the latter case the publication is done under a pseudonym.

In relation to personal data processed for archiving purposes in the public interest, Greek legislation make use of the opening clause of art. 89 par. 3 GDPR by regulating in art. 29 of L. 4624/2019 the processing of personal data for archiving purposes in the public interest. These are stated in their entirety below[135].

1. By way of derogation from Article 9(1) of the GDPR, the processing of special categories of personal data within the meaning of Article 9(1) of the GDPR shall be allowed where it is necessary for archiving purposes in the public interest. The controller shall have the

[135] Responses from NOA, KEMEA and HP to the questionnaire.

obligation to take suitable and specific measures to protect the data subject's legitimate interests. Such measures may include, as far as possible, in particular:

(a) access rights restrictions to controllers and processors;
(b) pseudonymisation of personal data;
(c) encryption of personal data;
(d) designation of a DPO.

2. By way of derogation from Article 15 of the GDPR, the data subject's right of access to data relating to him or her may be restricted where the exercise of that right is likely to render impossible or seriously impair the achievement of the objectives referred to in Article 9(1), and the exercise of the right would entail a disproportionate effort.

3. By way of derogation from Article 16 of the GDPR, the data subject shall not have the right to have the personal data relating to him or her rectified where the exercise of that right is likely to render impossible or seriously impair the achievement of the objectives referred to in (1) above or the exercise of the rights of others.

4. By way of derogation from subparagraphs (a), (b) and (d) of Article 18(1), and from Articles 20 and 21 of the GDPR, the rights of the data subject shall be restricted where their exercise is likely to render impossible or seriously impair the achievement of the objectives referred to in (1) above and where such limitations are deemed to be necessary for the achievement of such objectives.

These provisions apply only for Article's 9(2)(j) conditions. The rest of the provisions of Article 9(2) (a to i) are described in another article of the National Legislation.

Italy

As with all MS, Italy issued legislative decree no. 101/2018[136] to update their data protection code in line with the GDPR. Within Italy, the territorial scope of the GDPR mirrors that of Article 3, which thus applies as written in the GDPR. While some MS modify the opening clauses of Article 9(2)(j), Italy only modifies such clauses in respect of processing relating to specific aspects of health data that are not applicable to the programme of research with 7SHIELD.[137]

Spain

In Spain, Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights only refers in Article 26 to the processing of data for archiving purposes in the public interest by Public Administrations, without adding any exception to the rights of data subjects in this regard.

[136] Gazzetta Ufficiale (2018) Decreto Legislativo 10 Agosto 2018, n. 101 https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2018-09-04&atto.codiceRedazionale=18G00129&elenco30giorni=true

[137] Responses from ENG and SERCO to questionnaire and Practical Law - Italian Implementation of the GDPR (https://uk.practicallaw.thomsonreuters.com/w-019-8933) (last accessed: 22 April 2021)

Overall 7SHIELD will ensure that any processing of personal data is carried out in accordance with EU and national rules and restrictions where appropriate. Technical and organisational measures will be applied to ensure that all data is managed securely. This will be carried out in combination with the guidelines set out in the data management plan. Specifically, any personal data collected will be stored securely and only used for the purpose set out in the participant information sheets and the informed consent forms for each collection activity. Where possible all data will be anonymised where there is no requirement link the data to a specific person, in other cases data may also be pseudonymised to avoid identification of personal data. The EC[138] states that where it is necessary to retain a link between the research subjects and their personal data, wherever possible, the data should be pseudonymised in order to protect the data subject's privacy and minimise the risk to their fundamental rights in the event of unauthorised access. Data processed from the web and social media will be restricted, as far as possible, to information from organisations rather than individuals when conducting research related to warning messages. In the context of piloting activities, dummy or synthetic data will be used where possible.

6.2. Ethical considerations relating to piloting activities

The ALLEA code of conduct for research integrity[139] sets out the ethical principles for conducting ethical research. These principles are:

- Reliability – quality research through good design and methodology.
- Honesty – conducting all research in a fair, full and unbiased way.
- Respect – for all stakeholders and the research environment.
- Accountability – for all research, management, impacts, training and supervision.

The code of conduct sets out good practices for ethical research across all aspects. Research in 7SHIELD will strive achieve goals of ethical research from initial development to large scale piloting activities. Overall, 7SHIELD will ensure that aspects such as power relations, justice, fairness, right to non-social-sorting, right to create links with other human beings, and to be protected against harm will be embedded in research practices. The goal of all research in 7SHIELD is to ensure that while pushing forward the boundaries of innovative technology is not at the expense of the rights of individuals, groups or society at large but incorporates safeguarding measures and takes into account public concerns and perceptions.

In terms of the pilot use cases, in general there are not specific ethical consideration for each case beyond that can be addressed here beyond what has already been discussed

[138] https://ec.europa.eu/info/sites/info/files/5._h2020_ethics_and_data_protection_0.pdf

[139] ALLEA (2017) The European Code of Conduct for Research Integrity https://allea.org/wp-content/uploads/2017/05/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017.pdf

within this deliverable. However, in the context of other deliverables that cover the piloting activities in WP2 and WP8, ethical considerations will be included in a specific section within these deliverables to ensure that they are fully taken into account within the piloting process. Furthermore, given that each piloting site is a live and operational GS it means that piloting activities should not interfere with those operations. However, as above the details of the use cases themselves are classified documents it is not possible to discuss specific aspects in more detail in this deliverable and will be covered within other deliverables in WP2 and WP8.

7. Conclusions

7.1. Summary

In this deliverable we have reviewed the main applicable legal frameworks associated with the 7SHIELD project. This has included an extensive consideration of the implications of the GDPR, specific legislation at the EU level relating to activities within the 7SHIELD domain – the protection of critical infrastructure, the operation of ground space segments and cybersecurity. Then, within the scope of what is publicly available, the legal and ethical considerations relating to the development of the different 7SHIELD technologies components (across the prevention, detection, response and mitigation fields) and how they fit into existing legal frameworks, how 7SHIELD can assist organisations in maintain their compliance to these frameworks both for existing legislation and for legislation that will be implemented in the near future, and any legal restrictions directly related to development. Similarly, the ethical considerations associated to the development of such technology has been considered. Where possible this has covered both the development of technology in the research context and the potential deployment of such technology in an operation context following the project. Furthermore, in the context of the piloting activities, legal considerations for each pilot country have also been reviewed.

7.2. Next steps towards the final framework

This version of the deliverable covers only the preliminary version of the legal and ethical framework as applicable to 7SHIELD based on the initially proposed use cases, user requirements and technology development. Given the scope and scale of the system there will be many further requirements emerging as development and specifications are confirmed. This version has covered significant legislation at the EU level with some preliminary considerations at the national level. The next version of the framework will give a greater focus to national considerations and also significantly expand the ethical requirements associated with the technology development and the piloting activities. Where it is not possible to discuss in detail aspects relating to piloting activities or technology development – due to input from classified documents – these considerations will be embedded as far as possible within other deliverables in WP2 on user requirements and WP8 on piloting activities. Furthermore, such review and update of considerations will be addressed continually over the next year of the project to ensure they are embedded within the development process.

Annex I: End User Questionnaire

Preliminary ethics and legal framework questionnaire

This questionnaire is targeted towards end users and operators of pilot sites.

1. Article 9 of the GRPR refers to the processing of special categories of personal data. Articles 9(2)(j) and 89(2) provisions conditions for processing in relation to Archiving, Research and Statistics that MS could add restrictive applications to through the use of opening clauses. Does your country modify the opening clauses of these articles? Please provide details.

Answer

2. Are there any national laws relating to the use of CCTV and/or video surveillance in relation to data protection? Please provide details and an explanation

Answer

3. Are there any national laws relating to the operation of drones? Please provide details and an explanation

Answer

4. Are there any national laws relating to facial recognition? Please provide details and an explanation

Answer

5. Are there any special derogations relating to the personal data collection of biometric and health data (e.g., body temperature, heart rate, GPS position, etc.), this specifically relates to Article 9(4) in the GDPR. Please provide details and an explanation

Answer

6. Are there any specific legal frameworks relating to the operation of your Ground Segment in national law? Please provide details and an explanation

Answer

7. Are there any specific legal frameworks relating to the protection of national critical infrastructure in national law? Please provide details and an explanation

Answer

8. Is the NIS directive fully transposed into your national law? Are there any deviations? Please explain

Answer

9. Are you aware of any specific ethical considerations that could emerge from conducting your PUC? Please provide details and an explanation

Answer

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883284