Ref. Ares(2022)4083730 - 01/06/2022

# D9.2: Legal and Ethical Frameworks and Requirements



This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under Grant Agreement No 101021274

# Protection of Critical Infrastructures from advanced combined cyber and physical threats

| | |
|---|---|
| **Deliverable nº:** | D9.2 |
| **Deliverable name:** | Legal and Ethical Frameworks and Requirements |
| **Version:** | 1.0 |
| **Release date:** | 31/05/2022 |
| **Type* - Dissemination level**** | Report - Public |
| **Status:** | Final report |
| **Editors** | KUL |
| **Contributing WP** | WP9 |

**Abstract**

This deliverable is the outcome of the research as it is defined in the first task of WP9. More precisely, D9.2- Legal and Ethical Frameworks and Requirements represents the analysis of the relevant legal and ethical frameworks applicable to PRAETORIAN. The main aim of this deliverable is to identify the applicable legal and ethical principles and provide a high-level overview of the provisions which need to be considered in the development of PRAETORIAN technologies to assure that legal and regulatory standards are met. The D9.2 provides an overview of EU legislation on privacy and data protection, cybersecurity, and CIs (e.g., , the NIS Directive, GDPR, CI framework, etc.). Particular attention is given to the balancing of rights and interests, more specifically the rights of individuals (e.g., , the right to privacy and data protection) and society (e.g., , the protection of CIs). D9.2 builds on the previous analysis to provide a set of specific legal and ethical requirements and implementation guidelines, which will guide consortium members in their work and indicate ways to remedy the identified legal and ethical barriers.

**Type. Report; Demonstrator; Ethics **Dissemination Level. Public; Confidential (Confidential, only for members of the consortium (including the Commission Services)); RESTREINT UE (Classified information, RESTREINT UE (Commission Decision 2015/444/EC)).*

## Disclaimer

This document contains material which falls under the copyright of certain PRAETORIAN beneficiaries and may not be reproduced or copied without permission.

The information appearing in this document has been prepared in good faith and represents the views of the authors. Every effort has been made to ensure that all statements and information contained herein are accurate; however, the authors accept no statutory, contractual or other legal liability for any error or omission to the fullest extent that liability can be limited in law.

This document reflects only the view of its authors. Neither the authors nor the Research Executive Agency nor European Commission are responsible for any use that may be made of the information it contains. The use of the content provided is at the sole risk of the user. The reader is encouraged to investigate whether professional advice is necessary in all situations.

No part of this document may be copied, reproduced, disclosed, or distributed by any means whatsoever, including electronic without the express permission of the PRAETORIAN project partners. The same applies for translation, adaptation or transformation, arrangement or reproduction by any method or procedure whatsoever.

## PRAETORIAN

PRAETORIAN strategic goal is to increase the security and resilience of European CIs, facilitating the coordinated protection of interrelated CI against combined physical and cyber threats. To that end, the project will provide a multidimensional (economical, technological, policy, societal) yet installation-specific toolset comprising: (i) a Physical Situation Awareness system, (ii) a Cyber Situation Awareness system; (iii) a Hybrid Situation Awareness system, which will include digital twins of the infrastructure under protection; and (iv) a Coordinated Response system. The PRAETORIAN toolset will support the security managers of Critical Infrastructures (CI) in their decision making to anticipate and withstand potential cyber, physical or combined security threats to their own infrastructures and other interrelated CIs that could have a severe impact on their performance and/or the security of the population in their vicinity.

The project will specifically tackle (i.e.,, prevent, detect, response and, in case of a declared attack, mitigate) human-made cyber and physical attacks or natural disasters affecting CIs. It will also address how an attack or incident in a specific CI can jeopardise the normal operation of other neighbouring/interrelated CIs, and how to make all of them more resilient, by predicting cascading effects and proposing a unified response among CIs and assisting First Responder teams. PRAETORIAN is a CI-led, user-driven project, which will demonstrate its results in three international pilot clusters, some of them cross border -Spain, France and Croatia-, involving 9 outstanding critical infrastructures: 2 international airports, 2 ports, 3 hospitals and 2 power plants.

## Document history:

| Version | Date of issue | Content and changes | Partner |
|---|---|---|---|
| 0.1 | 12/04/2022 | Table of Contents | KUL |
| 0.2 | 12/05/2022 | First draft | KUL |
| 0.3 | 18/05/2022 | Continuous input | KUL |
| 0.4 | 24/05/2022 | Final draft for review | KUL |
| 1.0 | 31/05/2022 | Final version after review | KUL |

## List of Authors:

| Partner | Author |
|---|---|
| KUL | Maria Avramidou |
| KUL | Halid Kayhan |
| KUL | Jessica Schroers |
| KUL | Maja Nisevic |
| KUL | Bengi Zeybek |
| KUL | Anton Vedder |

**Peer reviewed by:**

| Partner | Reviewer |
|---|---|
| ETRA | Eva María Muñoz Navarro |
| EDF | Frederic Guyomard |
| DLR | Hilke Boumann |

# Contents

## Abbreviations and Acronyms

| Abbreviation | Description |
|---|---|
| **CCTV** | Closed-circuit television |
| **CER Directive** | Proposal for a Directive 2020/0365 of the European Parliament and of the Council on the resilience of critical entities, 16.12.2020. |
| **CFREU** | Charter of Fundamental Rights of the EU |
| **CIs** | Critical Infrastructures |
| **CJEU** | Court of Justice of the European Union |
| **CoE** | Council of Europe |
| **CSIRTs network** | Computer Security Incident Response Teams network |
| **Cybersecurity Act** | 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. |
| **DPIA** | Data Protection Impact Assessment |
| **DPO** | Data Protection Officer |
| **DSP** | Digital Service Providers |
| **EU** | European Union |
| **EUCC** | Common Criteria based European candidate cybersecurity certification scheme |
| **EC** | European Commission |
| **ECHR** | European Convention on Human Rights |

| Abbreviation | Description |
|---|---|
| **ECtHR** | European Court of Human Rights |
| **ECIs** | European Critical Infrastructures |
| **ECI Directive** | 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, OJ L 345/75, 23.12.2008. |
| **EDPS** | European Data Protection Supervisor |
| **ENISA** | European Union Agency for Network and Information Security. |
| **e-Privacy Directive** | Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector. |
| **e-Privacy Regulation** | Proposal for a Regulation 2017/0003 concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC. |
| **GDPR** | Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) |
| **ICT** | Information and Communication Technologies |
| **LED** | Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of |

| Abbreviation | Description |
|---|---|
| | criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/ 977/ JHA, (Law Enforcement Directive) |
| **NIS Directive** | Directive 2016/1148 on Network and Information Systems (hereinafter also NIS Directive. |
| **NIS2 Directive** | Directive 2020/0359 on measures for a high common level of cybersecurity, across the Union, repealing the Directive 2016/1148. |
| **OES** | Operators of Essential Services |
| **PRM** | Partner Relationship Management |
| **UAV** | Unmanned Aerial Vehicles |
| **UDHR** | Universal Declaration of Human Rights |
| **SOG-IS MRA** | Senior Officials Group Information Systems Security Mutual Recognition Agreement |
| **SOLAS Convention** | International Convention for the Safety of Life at Sea |
| **WP** | Work Package |

# Executive Summary

*Deliverable D9.2: Legal and Ethical Frameworks and Requirements,* together with the *Deliverable D9.1: Research Ethics and Privacy Management*, provides an analysis of the relevant legal and ethical frameworks applicable to PRAETORIAN technology throughout the project lifetime. More precisely, this document provides an overview of the international and the European Union frameworks on privacy and data protection, cybersecurity, critical infrastructures (CIs) and use of drones. Particular attention has been given to the balancing of the rights and interests, more specifically the rights of individuals (e.g., , the right to privacy and data protection) and a public interest in the protection of CIs. It also provides the consortium members an essential guidance on how to achieve the objectives of the PRAETORIAN research project in a legally compliant and ethically correct way. It should be highlighted that the use cases of the PRAETORIAN project and their specifications have not been finalised during the writing of this deliverable. Therefore, it was not possible to provide detailed specifications of referred legal requirements in the context of the project's use cases.

# 1. Introduction

## 1.1. Purpose of the document

The deliverable *D9.2: Legal and Ethical Frameworks and Requirements* – is the second report of the WP (Work Package) 9 of the PRAETORIAN project and aims to provide the essential legal and ethical frameworks and requirements that the consortium partners must follow to develop PRAETORIAN technology in compliance with legal and ethical frameworks. These frameworks and requirements represent a very wide spectrum, covering the fundamental rights of privacy and data protection and possible interferences with them, cybersecurity, protection of CIs and the use of drones. Together with the deliverable *D9.1: Research Ethics and Privacy Management*, which analysed the ethical framework, WP9 provides a guidance that is crucial throughout the project lifetime for the consortium to achieve the project objectives in a legally and ethically compliant way.

It is good to note that this deliverable contains legal instruments on an international level and on the level of the European Union for the subject matter of research. However, D9.2 does not cover research around national laws. Thus, consortium members should also consult the applicable national laws and apply them in conjunction with the legal instruments referred to in this document.
Since the use cases of PRAETORIAN project and their specifications have not been finalised, this affects the analysis provided in this deliverable and constitutes an obstacle to provide detailed and specific analysis of ethical and legal requirements in the context of the project's use cases.

## 1.2. Scope of the document

This document is aimed at the consortium partners to provide them with a brief overview of relevant EU and international legislation relating to the fundamental rights, processing of personal data, cybersecurity and security of Critical Infrastructures. It is also aimed at the European Commission to provide a detailed analysis of key aspects relating to the above issues in the context of the PRAETORIAN project.

## 1.3. Structure of the document

This document is structured as follows:

- Section 2 introduces an overview of the fundamental rights representing a particular importance in the context of the PRAETORIAN project, and how these rights can be limited.
- Section 3 provides an overview of the EU data protection legal regime.

- Section 4 focuses on the cybersecurity-related frameworks within the EU.
- Section 5 provides insights on the notion of CIs and European Critical Infrastructures (ECIs) and of the relevant legal frameworks.
- Section 6 gives a brief overview of the international and EU legal frameworks on the use of drones.

## 2. Fundamental Rights

The right to respect for private life (or the right to privacy) and the right to personal data protection are two closely related but separate rights. The right to privacy stems from the Universal Declaration of Human Rights (UDHR) adopted in 1948.[1] Shortly thereafter, the European Convention on Human Rights (ECHR), adopted in 1950 by the members of the Council of Europe (CoE), stipulated that everyone has the right to respect for their private and family life, home and correspondence. [2]

While Article 12 UDHR refers privacy as *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks"*,[3] Article 8 ECHR enshrines the right to respect for private and family life as follows:

> "*1. Everyone has the right to respect for his private life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*[4]

In the decades following the adoption of UDHR and ECHR, the emergence of the information society has brought many risks to the right to privacy in an individual's life. In order to mitigate these risks, regulations have been developed with a focus on personal data protection. At the EU level, data protection measures have been created since the 1970s, when some EU states began to adopt their relevant national laws. Data protection has evolved over the years into something of value in and of itself, rather than being part of the right to privacy. The EU legal order recognizes data protection as a fundamental right apart from the fundamental right to privacy.[5] This distinction is stipulated in Articles 7 and 8 of the Charter of Fundamental Rights of the EU (CFREU)[6] as follows:

> "***Article 7***
>
> ***Respect for private and family life***

[1] UN, Universal Declaration of Human Rights, 10 December 1948.
[2] Council of Europe, European Convention on Human Rights, 4 November 1950.
[3] See Article 12 UDHR.
[4] See Article 8 ECHR.
[5] EU Agency for Fundamental Rights, Handbook on European Data Protection Law, Luxembourg, Publications Office of the European Union, 2018, p. 18, 19.
[6] EU, Charter of the Fundamental Rights of the European Union, 26 October 2012.

*Everyone has the right to respect for his or her private and family life, home and communications.*

***Article 8***

***Protection of personal data***

*1. Everyone has the right to the protection of personal data concerning him or her.*

*2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*

*3. Compliance with these rules shall be subject to control by an independent authority.*"[7]

On the other hand, although a right to data protection is not included in the ECHR, a separate Convention of the Council of Europe, Convention 108,[8] addresses the protection of individuals with regard to automatic processing of personal data based on the same definition of personal data.[9]

The right to privacy relates to the cases where a private interest or private life (or family life) of an individual is jeopardized and this must be proven by the right holder. The right to personal data, on the other hand, relates to the circumstances under which personal data is processed, regardless of its relationship with or impact on privacy. From this aspect, the right to data protection is broader than the right to privacy. Privacy may be interfered with by personal data processing, but such an interference does not have to be proven in order for data protection regulations to be enforced.[10]

## 2.1. Interference with Privacy and Data Protection

To provide a background before diving into the interference with the fundamental rights, PRAETORIAN aims to enable the security stakeholders of the ECIs to manage the lifecycle of security threats, from the forecast, assessment and prevention to detection, response and mitigation, in a collaborative manner with the security teams from related CIs – being the CIs in a same or different sector. The strategic goal is to increase the security and resilience of ECIs, facilitating the coordinated protection of interrelated CIs against combined physical and cyber threats. For this purpose, the project will provide a multidimensional (i.e.,, economic, technological, policy and societal) yet installation-specific toolset comprising: (i) a Physical Situation Awareness system, (ii) a Cyber Situation Awareness system;

[7] See Articles 7 and 8 of CFREU.
[8] Council of Europe, The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), 28 January 1981.
[9] ibid, see Article 2(a).
[10] EU Agency for Fundamental Rights, Handbook on European Data Protection Law, Luxembourg, Publications Office of the European Union, 2018, p.20.

(iii) a Hybrid Situation Awareness system, which will include digital twins of the infrastructure under protection; and (iv) a Coordinated Response system. The project will test its toolset and demonstrate its results in three complementary and cross-site demonstrators organized by three international pilots, involving cross-border use cases (i.e.,, in Spain, France, and Croatia) through nine outstanding CIs: two international airports, two ports, three hospitals, and two power plants. The pilot sites will interact with each other, by providing feedback and lessons learned from one demo site to the others.

The components of the toolkit under development will gather data from both internal and external sources, which may include video footage from installed or mobile cameras, and from other comparable equipment such as cameras on Unmanned Aerial Vehicles (UAV). Furthermore, PRAETORIAN will deploy algorithms to detect and track vehicles and persons in near real-time, as well as to monitor activities in order to detect suspicious behaviour. The automated profiling and categorization of individuals presumed innocent based on their biometric data, as well as their potential automated profiling and categorization as suspicious or not, will interfere with the rights to privacy and data protection of the individuals concerned, including employees, passengers, and the general public in the CIs where the PRAETORIAN research activities will take place.

Both under the ECHR and CFREU, such interferences with fundamental rights are only possible when certain conditions are fulfilled. As quoted above, the second paragraph of Article 8 ECHR stipulates that,

> *"There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

This means that the right to respect for private life is not an absolute right and an interference with that right is allowed when such interference is:

- is in accordance with the law;
- pursues a legitimate aim;
- respects the essence of the fundamental rights and freedoms;
- is necessary and proportionate in a democratic society to achieve a legitimate purpose as listed.

On the other hand, Article 52(1) of CFREU on the "scope of guaranteed rights" stipulates,

> *"Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others"*

It is noteworthy that this provision is not only related to the rights to privacy or data protection but as a general provision related to all fundamental rights enshrined in the CFREU. Similarly to the above-mentioned provision of the ECHR, under the CFREU, any fundamental right, including rights to privacy and personal data protection, can be limited only if it:

- is in accordance with the law;
- respects the essence of the right; and
- is necessary and proportionate, in other words, appropriate to the specific objective of general interest they pursue.

It is worth explaining the main and common elements of these provisions. An interference, to be **in accordance with the law**, must have a legal basis. Indeed, several legislative instruments require the implementation of organizational and technological measures to maintain the security, availability, integrity, and confidentiality of personal data, as well as network and information systems. Moreover, each Critical Infrastructures (CIs) sector-specific framework (e.g., transport, health, energy, and finance) imposes further requirements, such as the SOLAS Convention,[11] regulating the security measures for the protection against physical and cyber threats in the context of ports. Thus, limitations on the rights to privacy and data protection as part of the PRAETORIAN project activities, at first place, seem to be in accordance with the law. However, further assessment on a case-by-case basis should be made to ensure that there is always a legitimate basis.

**Respecting the essence of the right** means limitations that are so extensive and intrusive that they deprive a fundamental right of its basic content cannot be justified. The limitation will be unlawful whenever the essence of the right is compromised – regardless of whether it achieves an objective of general interest and meets the criteria of necessity and proportionality.[12]

If certain measures are needed in order to achieve a particular public interest, a limitation may be **necessary**; nevertheless, necessity, as defined by the Court of Justice of the European Union (CJEU),

[11] International Convention for the Safety of Life at Sea (SOLAS), 1 November 1974.
[12] EU Agency for Fundamental Rights, Handbook on European Data Protection Law, Luxembourg, Publications Office of the European Union, 2018, p.44.

also entails that the measures implemented must be less intrusive than other possibilities for accomplishing the same goal. The CJEU applies a strict necessity test to limitations on the rights to respect for private life and protection of personal data, concluding that "*derogations and limitations must apply as insofar as strictly necessary.*"[13] If a limitation is found strictly necessary, it must also be evaluated to see if it is proportional.[14]

**Proportionality** indicates that the benefits of the limitations should balance the negative effects that it has on the enjoyment of the fundamental rights in question.[15] Limitations must include sufficient measures to reduce disadvantages and dangers to the enjoyment of privacy and data protection rights.[16]

From a more practical perspective, factors such as potential threats, risks, harms, and benefits must be considered while evaluating the appropriateness and effectiveness of a security measure. Furthermore, the security measure at issue must be required in the sense that there are no alternative less invasive options. This means that the presence (or lack thereof) of alternative but equally effective measures to accomplish the desired goal should be confirmed. Finally, the specific security measure should not go beyond, in order to be proportionate, what is reasonable and required to achieve the precise lawful goal it is pursuing.[17] For instance, while CCTV cameras have been shown to be an efficient way of monitoring for the rapid identification of various threats and, thus, been used commonly-, not all sections of the CIs in question require the same level of intrusiveness when it comes to the processing and analysis of the data from cameras.[18] According to European Data Protection Board (EDPB), besides all the measures and their combination that will be implemented, including the goals they seek to achieve, they must be explained clearly and adequately.[19]

In addition to EDPB, the CJEU and the European Court of Human Rights (ECtHR) interpreted the principle of proportionality in the context of processing personal data deriving from the surveillance

[13] C-362/14 Maximillian Schrems v Data Protection Commissioner, 06 October 2015, ECLI:EU:C:2015:650 ("Schrems"), para.92.
[14] EU Agency for Fundamental Rights, Handbook on European Data Protection Law, Luxembourg, Publications Office of the European Union, 2018, p.46.
[15] European Data Protection Supervisor (2017), Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit.
[16] EU Agency for Fundamental Rights, Handbook on European Data Protection Law, Luxembourg, Publications Office of the European Union, 2018, p.46.
[17] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, 536/14/EN, WP 21, Brussels, 27 Feb 2014.
[18] O. Mironenko Enerstvedt, Aviation Security, Privacy, Data Protection and other Human Rights: Technologies and Legal Principles, SPRINGER, Law, Governance and Technology Series, Sub-series: Issues in Privacy and Data Protection 37, 2017, p.183.
[19] European Data Protection Supervisor (2017), Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit.

of the masses and provided specific criteria that must be met by those security measures of surveillance.[20] In the pursuit of a balance between security and the fundamental rights to privacy and data protection, these criteria provided by the CJEU and the ECtHR outline the concept of proportionality. First of all, objective criteria must be established for restricting data access, such as a pre-determined number and position of people having access authorization, as well as for the future use of such data being clearly and strictly limited to the objectives for which access authorization was provided. The use of data must be limited to the security objective for which it was collected, and as such, capable of justifying the interference that its use involves. It is also critical that the implementation of such measures be overseen by a supervisory authority. Furthermore, during the time that the data is held in the databases, in order to ensure the security and protection of the data, adequate organizational and technological measures must be put in place. In addition, rules must be established for the deletion or destruction of transferred personal data when it is no longer required. However, it should be noted that the CJEU, in its *Opinion 1/15* which is dated 26 July 2017, agreed that an extension of the period of time of retention is reasonable on the basis of the typical lifetime of international serious crime networks and the duration and complexity of investigations pertaining to those networks.[21] Lastly, except in cases of validly established urgency, access by competent national authorities, such as law enforcement agencies, to private-sector databases, such as port authority databases, should be subject to a prior review or authorization carried out either by a judicial or, in any case, an independent authority, and that the decision of that court or body should be made following a reasoned request by those authorities.[22]

[20] Cases: CJEU: C-293/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, 8 April 2014, ECLI:EU:C:2014:238 ("Digital Rights Ireland"), C-362/14 Maximillian Schrems v Data Protection Commissioner, 06 October 2015, ECLI:EU:C:2015:650 ("Schrems"), C-203/15 and C-698/15 Tele2 Sverige AB v Postoch telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, 21 December 2016, ECLI:EU:C:2016:970 ("Tele2"), Opinion 1/15 26 July 2017, ECLI:EU:C:2017:592 ("Opinion 1/15"), ECtHR: Case of Roman Zakharov v. Russia, App. No 47143/06, 04 December 2015, ECLI:CE:ECHR:2015:1204JUD004714306 ("Zakharov") and Case of Szabó and Vissy v. Hungary, App. No 37138/14, Final Text 06 June 2016, ECLI:CE:ECHR:2016:0112JUD003713814 ("Szabó").
[21] CJEU: Opinion 1/15, 26 July 2017, ECLI:EU:C:2017:592.
[22] Plixavra Vogiatzoglou, Anton Vedder, SAURON Deliverable D3.5 Legal Requirements Specifications (2018), p.11, p. 12.

# 3. EU Data Protection Framework

## 3.1. The General Data Protection Regulation

Since 25 May 2018 the General Data Protection Regulation (GDPR)[23] is applicable. This chapter will give an overview on the relevant provisions of the GDPR when it comes to PRAETORIAN project. The GDPR, as a Regulation, is directly applicable in the Member States. Nevertheless, for a number of provisions, it is explicitly foreseen that Member States' laws are allowed to diverge from the GDPR.

### 3.1.1 Does the GDPR apply to the processing in PRAETORIAN?

To identify whether the GDPR is applicable, the material and the territorial scope needs to be considered.

#### 3.1.1.1 Material scope

The GDPR applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.[24] However, the GDPR does not apply to activities outside the scope of Union law, Member States activities around foreign and security policy, processing by competent authorities in criminal offences and public security and in case of personal or household activities of natural persons. [25]

**Personal data**

According to the GDPR, personal data means any information relating to an identified or identifiable natural person ('data subject').[26] In addition, 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.[27] In case data is properly anonymized, the data protection legislation does not apply, as the data does not relate to an identified or identifiable natural person anymore.[28] However, the threshold for anonymization is rather high. Pseudonymization, even though it is often confused with anonymization,

[23] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016.
[24] See Article 2 (1) GDPR.
[25] See Article 2 (2) GDPR.
[26] See Article 4 (1) GDPR.
[27] See Article 4 (1) GDPR.
[28] Recital 26 GDPR.

is different from anonymization. As defined in Article 4 (5) pseudonymization 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 organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person". Pseudonymized data still falls in the scope of the Regulation and the data protection provisions need to be adhered to.

**Data processing**

Data processing refers to any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means. [29] The scope of processing is quite broad and includes all kind of operations 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. [30]

**Wholly or partly by automated means**

Wholly or partly by automated means entails that the GDPR applies to any processing of personal data as soon as it is (even partially) done with the help of for example a computer, mobile device or any other automated device. [31] Even if no automated means are used, the GDPR is applicable if the data is included in a manual filing system or is intended to form part of such a system.[32]

**Exceptions**

The GDPR does not apply to activities outside the scope of EU law, Member States activities in foreign and security policy, processing by competent authorities around criminal offences and public security and in case of personal or household activities of natural persons.[33]

Most of these exceptions will not be relevant for PRAETORIAN. However, processing by competent authorities in criminal offences and public security could potentially apply in certain cases.

| Would PRAETORIAN be used by parties which can be considered a competent authority within the meaning of the Law Enforcement Directive (LED)? [34] |
|---|

[29] See Article 4 (2) GDPR.
[30] See Article 4 (2) GDPR.
[31] See Article 2(1) GDPR.
[32] See Article 2(1) GDPR.
[33] Article 2 (2) GDPR.
[34] Article 2 LED.

#### 3.1.1.2 Territorial scope

The GDPR applies to the processing of personal data in the context of activities of an establishment of a controller or a processor in the EU.[35] It is not important whether that processing takes place in the EU.[36] Furthermore, even if the controller or processor are not established in the EU, the GDPR applies in case of the offering of goods or services to data subjects in the EU, or in case of monitoring of the behaviour of data subjects, if this behaviour takes place within the EU.[37]

**Controller** refers to 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. [38]

**Processor** refers to a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. [39]

| Would the party using PRAETORIAN be established in the EU or monitor the behaviour of data subjects in the EU?<br>- It is assumed that the PRAETORIAN technology will be used by CIs in the EU |
|---|

### 3.1.2 What personal data can be processed?

As explained above, personal data means any information relating to an identified or identifiable natural person. Certain categories of personal data are considered special categories of personal data and receive special protection. These are personal data which reveal or are:[40]

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation

[35] Article 3 (1) GDPR.
[36] Article 3 (1) GDPR.
[37] See Article 3 (2) GDPR.
[38] See Article 4 (7) GPDR.
[39]Article 4 (8) GDPR.
[40] Article 9 GDPR.

| CASE | REQUIREMENT |
|---|---|
| The PRAETORIAN technology tool and research activities will process personal data | It must be identified what personal data will be processed in the PRAETORIAN technology tool, research, validation and demonstration activities e.g., , by the Social Media Integration Module, Video analytics |
| The PRAETORIAN technology tool and research activities will process special categories of personal data | It must be identified whether special categories of personal data will be processed by the PRAETORIAN technology tool and research activities |

### 3.1.3 Who is controller and processor?

It is important to establish who is the controller of data processing and whether or not processors are involved in the processing. This subsection will explain the definition and allocation of the roles of controller and processor.

#### 3.1.3.1 Identifying controllers

Establishing who is controller is important since the controller is the one who is responsible for the processing activities and the main addressee of the GDPR. The data controller is the "natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".[41]

**Determining purposes and means**

In case the purposes and means are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided by law.[42]

In general, however, the allocation of the notion of controller is based on its concrete activities in a specific context. It should be noted that the assessment of the status is based upon a factual

[41] Article 4 (1) GDPR.
[42] See Article 4 (7) GDPR.

assessment, depending on who determines the purposes and means. Contractual arrangements can only provide an indication and always need to be checked against the factual circumstances.[43]

**Alone or jointly with others**

It is also possible that several controllers are involved in a data processing. In case they jointly determine the purposes and means of processing, they are considered joint controllers.[44] In case of joint controllership, the controllers are obliged to make an arrangement between them, specifying their respective roles and responsibilities, in particular towards the data subject as they have to ensure the exercise of the data subject rights and information duties.[45]

As explained by the EDPB, joint participation can be in different forms, it can be for example in the form of a common decision or can result from converging decisions of the controllers regarding the purposes and essential means.[46] A common decision is the traditional understanding of joint control whereby the controllers decide together, while the case of converging decisions arises from the case law of the CJEU, in particular *Wirtschaftsakademie*[47], *Jehovan todistajat*[48] and *Fashion ID*[49]. If controllers do not take joint decisions, but the decisions they take are converging on purposes and means since they complement each other and "*are necessary for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of the processing*"[50] they are considered to be converging decisions.[51] In these cases, the controllers are joint controllers, in respect of those operations for which they determine jointly the means and purposes of the processing.

#### 3.1.3.2 Identifying processors

The processor is the "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".[52] The processor is always acting under the authority of the

[43] European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' (2.9.2020) 9.
[44] See Article 26 (1) GPDR.
[45] Article 26 GDPR.
[46] European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' (2.9.2020), p.18.
[47] CJEU 5 June 2018, C-210/16, ECLI:EU:C:2018:388 ('Wirtschaftsakademie Case').
[48] CJEU 10 July 2018, C-25/17, ECLI:EU:C:2018:551 ('Jehovan todistajat case').
[49] CJEU 29 July 2019, C-40/17, ECLI:EU:C:2019:629 ('Fashion ID case').
[50] European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' (2.9.2020), p. 18
[51] European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' (2.9.2020), p.18.
[52] See Article 4 (8) GDPR.

controller, as soon as the processor processes the data for their own purposes and determine their own means, it would be considered a controller.

Accordingly, the same entity may act at the same time as a controller for certain processing operations and as a processor for others and the qualification as controller or processor should be assessed with regard to specific sets of data or operations.[53]

This is how it is considered within the PRAETORIAN area:

| **CASE** | **REQUIREMENT** |
|---|---|
| The PRAETORIAN technology tool and research activities will process personal data | When using the PRAETORIAN technology tool and for research activities the controllers must be identified and aware of their responsibilities |
| The PRAETORIAN technology tool and research activities will process personal data and processors will be used | When using the PRAETORIAN technology tool and research activities, the processors must be identified and controller-processor agreements established |

### 3.1.4 Data controller's obligations

It is important to identify the controller, as the controller is the responsible entity for compliance with data protection legislation. Some obligations that the controller must fulfil are:

| |
|---|
| • The controller must ensure compliance with the GDPR principles (Article 5 GDPR) |
| • The controller must ensure the existence of an appropriate lawful basis for the processing (Article 6 GDPR) |
| • If processing is based on consent, the controller must ensure a procedure to gather and manage consent of the data subjects (Article 7 GDPR) |
| • The controller must ensure the information of data subjects (Articles 12-14 GDPR) |
| • The controller is the one responsible for the follow-up and effectively addressing of data subjects' requests concerning the exercise of their rights (Articles 12-22 GDPR) |

[53] European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' (2.9.2020), p.11.

| |
|---|
| • The controller must make contracts to regulate its relationship with processors (Article 28 GDPR) |
| • The controller must keep records of processing activities (Article 30 GDPR) |
| • The controller must take adequate security measures to apply to the means of processing (Article 32 GDPR) |
| • The controller should have a procedure to manage personal data breaches and notify the Data Protection Authority and data subjects where necessary (Articles 33-34 GDPR). |

The main aim is to ensure a complete and effective protection of the data subject.[54]

#### 3.1.4.1 The controller has to ensure compliance with the GDPR principles

**Identifying the purpose of the processing**

The controller is the one who determines the purpose of the processing. This purpose is important for various requirements of the GDPR, including for compliance with its principles. Therefore, it should be clear from the outset why the personal data will be processed.

| CASE | REQUIREMENT |
|---|---|
| For the purpose of the PRAETORIAN research activities personal data will be processed | The purpose of each processing of personal data in the PRAETORIAN technology tool and research activities must be identified, including exposing and discussing it with all the WP leaders and task leaders of PRAETORIAN. |

**Lawfulness, fairness and transparency**

The GDPR in its Article 5, has defined the essential principle that covers lawfulness, fairness and transparency, when it comes to data processing. Even though it is mentioned as a single principle, it has three different components.

[54] See e.g., , CJEU Case C-131/12 Google Spain and Google [2014] EU:C:2014:317, para 34; CJEU Case C-210/16, Wirtschaftsakademie Schleswig-Holstein [2018] ECLI:EU:C:2018:388 para 28.

**Lawfulness** means that the processing of personal data can only take place if covered by a 'legal basis'. The GDPR lists six legal bases in Article 6 GDPR on which controllers can rely to process personal data. These legal bases are the well-known consent, but also processing necessary for the performance of a contract, for compliance with a legal obligation or to protect vital interests of the data subject or another natural person can be a lawful basis for the processing of personal data.[55] Furthermore, the processing can be based on the reason that it 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, or that it is necessary for the purposes of the legitimate interest pursued by the controller or by a third party.[56] In order to use legitimate interest as a legal basis, it is, however, necessary to balance it against the fundamental rights and freedoms of the data subject.

**Fairness** requires controllers to handle personal data in ways that individuals reasonably expect them to do so, and to take into consideration the interests and reasonable expectations of individuals.

**Transparency** puts a duty on data controllers to be open and clear about the processing of personal data they carry out.

| **CASE** | **REQUIREMENT** |
|---|---|
| The PRAETORIAN technology tool and research activities will process personal data | The legal ground for each processing of personal data in the context of PRAETORIAN technology tool, research, validation and demonstration activities must be established |
| The PRAETORIAN technology tool and research activities will process personal data | When developing the PRAETORIAN technology the interests and reasonable expectations of the data subjects should be taken into account |
| The PRAETORIAN technology tool and research activities will process personal data | The PRAETORIAN technology should allow the controllers to be transparent about the processing of personal data as far as possible |

[55] Article 6 (1) (a), (b), (c) and (d) GDPR.
[56] Article 6 (1) (e) and (f) GDPR.

**Purpose limitation**

The principle of purpose limitation requires that data are only processed for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with the initial purposes.

| CASE | REQUIREMENT |
|---|---|
| The PRAETORIAN technology tool and research activities will process personal data | The identified purpose should be specific, explicit and legitimate |
| The PRAETORIAN technology tool and research activities will process personal data | The system should be designed in a way that only the relevant data for that purpose will be processed |
| The PRAETORIAN technology tool and research activities will process personal data | When developing the system, it should be ensured that the personal data are not further processed in a manner incompatible with the initial purpose of the processing |

**Data minimisation**

According to the data minimisation principle, only the minimum data needed to achieve the purpose set by the controller must be processed. This means that already during the collection only the relevant data for the purpose will be collected, and that, as soon as data is not relevant for the purpose anymore, it will be deleted. This also means that for example if it would be possible to use anonymized or pseudonymized data to achieve the purpose, then the data should be anonymized or pseudonymized.

| CASE | REQUIREMENT |
|---|---|
| The PRAETORIAN technology tool and research activities will process personal data | The tools must only collect the minimum personal data necessary to achieve the purpose |
| The PRAETORIAN technology tool and research activities will process personal data | If possible, the data should be pseudonymized or anonymized |

**Accuracy**

The data accuracy principle requires that the personal data should be accurate and kept up to date. The controller should take every reasonable step to ensure that personal data that are inaccurate are erased or rectified without delay.

| CASE | REQUIREMENT |
|---|---|
| The PRAETORIAN technology tool and research activities will process personal data | The tools should allow to verify that personal data is accurate and be able to correct and update personal data |

**Storage limitation**

The principle of storage limitation requires that personal data should not be kept longer than necessary for the processing purposes. The data might be kept longer for archiving, scientific or historical research purposes, but then it needs to be ensured that the rights and freedoms of the data subject are safeguarded.

| CASE | REQUIREMENT |
|---|---|
| The PRAETORIAN technology tool and research activities will store personal data | Personal data should be deleted when they are not necessary anymore to fulfil their processing purpose |

**Integrity and confidentiality**

The principle of integrity and confidentiality requires the personal data to be secured. When processing personal data, appropriate technical or organizational measures should be taken to ensure protection against unauthorised or unlawful processing, access, disclosure/accidental loss, destruction or damage.

| CASE | REQUIREMENT |
|---|---|
| The PRAETORIAN technology tool and research activities will process personal data | The technology must be designed and implemented in such a way that the personal data are secure and protected against |

| | |
|---|---|
| | unauthorised or unlawful processing, loss, destruction or damage.<br>Measures include for example the pseudonymization and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.[57] It must also be ensured that any natural person under the authority of the controller (or the processor) who has access to personal data does not process it outside of legal obligations or the instructions from the controller. Each partner within the PRAETORIAN project is responsible to apply the adapted measures in accordance with the Processor recommendations. |

**Accountability**

The principle of accountability entails that the controller is responsible and must be able to demonstrate compliance with the abovementioned principles. Within the GDPR this principle is for example enshrined in the obligations for the controller such as that the controller must implement appropriate technical and organizational measures to ensure and be able to demonstrate compliance with the GDPR, i.e.,, Article 24 , the obligation regarding data protection by design and default, i.e.,, Article 25 or the obligation to keep records of processing activities, i.e.,, Article 30 GDPR.

[57] See Article 32 (1) GDPR.

| CASE | REQUIREMENT |
|---|---|
| For the purpose of the research in the PRAETORIAN project personal data will processed | The technology tool must be designed in such a way that the controller is able to demonstrate compliance with the GDPR |

#### 3.1.4.2 The controller has to ensure the existence of an appropriate legal ground for the processing

One of the controller's obligations is to ensure that personal data is processed lawfully by basing all processing on a legal ground.

The GDPR in its Article 6, provides six potential legal grounds to lawfully process personal data:

(a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;

(b) the 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;

(c) the processing is necessary for **compliance with a legal obligation** to which the controller is subject;

(d) the processing is necessary in order to **protect the vital interests** of the data subject or of another natural person;

(e) the 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;

(f) the 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.

| CASE | REQUIREMENT |
|---|---|
| The PRAETORIAN technology tool and research activities will process personal data | The legal basis of each processing of personal data must be established |

**Special categories of personal data**

As explained above, in the GDPR are certain categories of personal data considered as special. The processing of these categories of data is in principle prohibited due to their sensitive character.

Exceptions to the prohibition of processing of these special categories of personal data exist and they are listed in Article 9 (2) GDPR. These exceptions are cumulative with the legal grounds of Article 6 GDPR.

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subject;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

| **CASE** | **REQUIREMENT** |
|---|---|
| For the purpose of the research in the PRAETORIAN project special categories of personal data will be processed | The legal basis of the processing should be established and it must be established if one of the exceptions to the prohibition of processing is applicable |

#### 3.1.4.3 The controller has to inform data subjects

When a controller processes personal data, whether obtained directly from the data subject, or indirectly from somewhere else, the data subject must be informed of the processing. This information, as well as information relating to the exercise of data subject rights, must be in a concise, transparent, intelligible and easily accessible form, using clear and plain language.[58] The list below gives an overview of the information which should be provided to the data subject. In case the personal data are collected from the data subject, the information should be provided at the moment when the personal data are collected. In case the personal data are not obtained from the data subject, the controller should provide the information within a reasonable period after obtaining the personal data, but at the latest within one month.[59] In case the personal data are to be used for communication with the data subject, the information should be provided at the latest at the time of the first

[58] See Article 12 GDPR.
[59] See Article 14 (3) (a) GDPR.

communication to that data subject; or if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.[60]

| **Directly from the data subject (art. 13 GDPR)** | **Indirectly (art. 14 GDPR)** |
|---|---|
| Identity and the contact details of the controller / the controller's representative; | |
| Purposes & legal basis | |
| The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period | |
| | The categories of personal data concerned |
| Information on data subject rights | |
| The right to lodge a complaint with a supervisory authority; | |
| | Source of personal data (publicly accessible sources?) |
| Statutory or contractual requirement/requirement necessary to enter into a contract, obligation to provide the personal data and the possible consequences of failure to provide such data? | |
| [DPO] Contact details of the DPO | |
| [Based on legitimate interest] The legitimate interest | |
| [Other recipients] Recipients or categories of recipients of the personal data | |

[60] See Article 14 (3) (b) and (c) GDPR.

| |
|---|
| [Transfers] That it will be transferred & information on adequacy decision or safeguards |
| [Consent] The existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal |
| [Automated decision-making] The existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences for the data subject |

In case of further processing of the personal data for another purpose than the one for which the personal data were obtained, the controller should provide the data subject with information on that other purpose before the processing.

It is not necessary to inform the data subject in case:

- The data subject already has the information;
- The provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or in case the information provision is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
- Obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides for appropriate measures to protect the data subject's legitimate interests;
- Where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

| **CASE** | **REQUIREMENT** |
|---|---|
| For the purpose of the research in the PRAETORIAN project personal data will be processed | Data subjects must be informed of the processing of their personal data, including al |

| | |
|---|---|
| | the research activities as well piloting of the project |

#### 3.1.4.4 The controller is the one responsible for the follow-up and effectively addressing of data subjects requests concerning the exercise of their rights

Data subjects have certain rights towards the data controllers.[61] These rights are:

| | |
|---|---|
| Right to information | Articles 12, 13 and 14 GDPR |
| Right of access | Article 15 GDPR |
| Right to rectification | Article 16 GDPR |
| Right to erasure ("right to be forgotten") | Article 17 GDPR |
| Right to restriction of processing | Article 18 GDPR |
| Right to data portability | Article 20 GDPR |
| Right to object | Article 21 GDPR |
| Right not to be subject to automated decision making | Article 22 GDPR |

In order to be able to abide these rights, the controller must:

- Have a contact point that is known and can be easily reached by the data subject
- Be able to give access to the data relating to the data subject
- Be able to adjust, erase, restrict the processing and port the personal data
- Notify third parties who have received or seen the personal data
- Give an answer to the data subject without undue delay and at the latest within one month of receipt of the request

[61] The data subject rights may be restricted by Union or Member State law. However, they may only restricted when specific interests are at stake, which are exhaustively listed in Article 23 (1) GDPR (EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR, Version 2.0, adopted on 13 October 2021, p. 6.).

| CASE | REQUIREMENT |
|---|---|
| The PRAETORIAN technology tool and research activities will process personal data | The PRAETORIAN technology tool and research activities must be able to comply with the data subjects rights |
| The PRAETORIAN technology tool and research activities will process personal data | The controller using the PRAETORIAN technology should have a contact point that is known and can be easily reached by the data subject |
| The PRAETORIAN technology tool and research activities will process personal data | The PRAETORIAN technology tool and research activities should be able to give access to the data relating to the data subject., when the personal data has not been anonymised |
| The PRAETORIAN technology tool and research activities will process personal data | The PRAETORIAN technology tool and research activities should be able to adjust, erase, restrict the processing and modify the personal data |
| The PRAETORIAN technology tool and research activities will process personal data and will share it with third parties | The controller using the PRAETORIAN technology should be able to notify third parties who have received or seen the personal data |
| The PRAETORIAN technology tool and research activities will process personal data | The controller using the PRAETORIAN technology should be able to answer the request of the data subject without undue delay and at the latest within one month of receipt of the request |

**Automated decision-making**

The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.[62] It is nevertheless allowed[63], if the decision-making is necessary for entering into, or performance of a contract between the data subject and a data controller; or is based on the data subject's explicit consent. In those cases the data controller has to implement suitable measures to

[62] Article 22 (1) GDPR.
[63] Except for special categories of data, see Article 22 (4) GDPR.

safeguard the data subject's rights and freedoms and legitimate interests.[64] The minimum is to be able to obtain human intervention on the part of the controller so that the data subject can express his or her point of view and to contest the decision.[65] Finally, it is allowed in case it is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.[66]

In case PRAETORIAN will process personal data in such a way that it could fall under the category of profiling (automated processing of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements" [67] ) the prohibition of automated individual decision-making would apply. In that case it would need to be assessed whether one of the exceptions is applicable, or to be ensured that the decision is not "solely automated".

#### 3.1.4.5 The controller has to make contracts to regulate its relationship with processors

When the controller uses the services of processors, it is important that the controller will only use processors which provide sufficient guarantees for compliance with the GDPR.[68] Furthermore, the controller must conclude a contract with the processor which is binding and which sets out the subject-matter and duration of the processing, the nature and the purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.[69]

| CASE | REQUIREMENT |
|---|---|
| Processors are necessary for the processing in the PRAETORIAN technology tool and research activities | It must be established that the processors provide sufficient guarantees that they comply with the GDPR<br>Adherence to an approved code of conduct or approved certification mechanism could be an element to demonstrate sufficient guarantees (art. 28 (5) GDPR) |

[64] Article 22 (2) (a) and (c), Article 22 (3) GDPR.
[65] Article 22 (3) GDPR.
[66] Article 22 (2) (b) GDPR.
[67] Article 4 (4) GDPR.
[68] Article 28 (1) GDPR.
[69] Article 28 (3) GDPR.

| | |
|---|---|
| Processors are necessary for the processing in the PRAETORIAN technology tool and research activities | Controller-processor contracts must be concluded. These contracts should be separate and distinct from the possible other types of contracts between the same parties, e.g., employment contracts, etc. |

#### 3.1.4.6 The controller has to keep records of processing activities

The controller, needs to maintain records of the processing activities, and be able to make these records available to the supervisory authority on request.[70] Except in case of the processing of special categories of data, personal data relating to criminal convictions and offences or processing that is likely to result in a risk to the rights and freedoms of data subjects, there is an exception of this obligation for organisations employing less than 250 persons.[71]

The records can be in electronic form but should be in writing.[72] The information included should be:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in case necessary, the documentation of suitable safeguards;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures.

| **CASE** | **REQUIREMENT** |
|---|---|
| The PRAETORIAN technology tool and research activities will process personal data | The PRAETORIAN technology tool and research activities should provide information that the |

[70] Article 30 GDPR.
[71] Article 30 (5) GDPR.
[72] Article 30 (3) GDPR.

| | |
|---|---|
| | controller using it can have the required records of the processing activities |

#### 3.1.4.7 The controller has to take adequate security measures to apply to the means of processing

The controller (as well as the processor) has to implement appropriate technical and organisational measures to secure the personal data, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.[73] Whether the measures are appropriate depends on the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. [74] These measures include for example the pseudonymization and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.[75] It must also be ensured that any natural person under the authority of the controller (or the processor) who has access to personal data does not process it outside of legal obligations or the instructions from the controller. [76]

#### 3.1.4.8 The controller should have a procedure to manage personal data breaches and notify the Data Protection Authority and data subjects where necessary

Notwithstanding the taken security measures, it might happen that the security is breached. In such a case the controller must without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority.[77] In case the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall also communicate the personal data breach to the data subject without undue delay.[78]

[73] Article 32 GDPR.
[74] Article 32 (1) GDPR.
[75] Article 32 (1) GDPR.
[76] Article 32 (4) GDPR.
[77] Article 33 GDPR.
[78] Article 34 GDPR.

| CASE | REQUIREMENT |
|---|---|
| The PRAETORIAN technology tool and research activities will process personal data and a data breach occurs | In case of a data breach it must be possible to notify the supervisory authority within 72 hours and provide information on the data breach |

**Data Protection Officer**

In case:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences then a Data protection officer (DPO) needs to be designated.[79]

The main tasks of the DPO are to inform the data controller on their obligations and to assist in complying with the GDPR obligations.

| CASE | REQUIREMENT |
|---|---|
| The controller needs to appoint a DPO | A DPO must have the possibility to evaluate the PRAETORIAN technology |

## 3.2. E-Privacy Directive

The Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive) regulates the processing of personal data and the protection of privacy in the electronic communications. It aims to the free movement of such data and of electronic communication equipment and services in the EU.[80]

A revision of the e-Privacy Directive and the Proposal for the Regulation 2017/0003 concerning the respect for private life and the protection of personal data in electronic communications and repealing

[79] Article 37 GDPR.
[80] See Article 1, e-Privacy Directive.

Directive 2002/58/EC (e-Privacy Regulation) were announced. However, due to a lack of political compromise the e-Privacy Regulation has not entered into the force, yet. [81] Therefore there is, still, no replacement of the e-Privacy Directive.[82]

The e-Privacy Directive , is *lex specialis* to the GDPR, which means that in case of a potential conflict among the two legal frameworks the e-Privacy Directive overrides the GDPR.

The uncertainty on the adoption of an e-Privacy Regulation could potentially play an important role, in case of the application of the PRAETORIAN technology within the electronic communications industry. In that case, additional requirements may have to be met and end-users should take into account the uncertainty regarding the adoption of the new e-Privacy Regulation.

## 3.3. Law Enforcement Directive

As explained above, the GDPR does not apply to processing by competent authorities in the area of criminal offences. This type of processing is covered by the Law Enforcement Directive (LED)[83], which accompanies and complements the GDPR. As a Directive, it needs to be implemented in Member States' legislation. The LED applies to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.[84] Like the GDPR, it applies to the processing of personal data wholly or partly by automated means, and to the processing of personal data by non-automated means which form part, or are intended to form part, of a filing system, but it does not apply to activities which fall outside the scope of Union law or activities by the Union institutions, bodies, offices and agencies.[85] To assess whether the LED is applicable, two aspects are important: the purpose of the processing and the notion of 'competent authorities'. Competent authorities are (a) any public authority competent for the

[81] Proposal for a Regulation 2017/0003 concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) ("e-Privacy Regulation").
[82] According to the proposal for an e-Privacy Regulation, it will apply to new players providing electronic communication services. In addition, it establishes stronger rules for the protection of electronic communications of people and businesses and guarantees privacy for content and metadata. Moreover, it urges new business opportunities, establishes new rules on cookies; and it offers protection against spam, and it provides for more effective enforcement regime compared to the one provided under the e-Privacy Directive.
[83] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/ 977/ JHA, OJ L 119, 4.5.2016 (LED).
[84] Article 2 (1) jo. Article 1 (1) LED.
[85] Article 2 (2) and (3) LED.

prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or (b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.[86] The purpose of the processing by these competent authorities is the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.[87] In case Member State law entrusts the entities using the PRAETORIAN solution to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and preventing of threats to public security, then, for those specific activities, the LED would apply.

## 3.4. The Regulation 2018/1807 on the Free-Flow of Non-Personal Data

Across the EU, there is plenty of national legislation that creates technological and legal impediments to the free flow of non-personal data. Non-personal data refers to information that does not identify a natural person, such as environmental, industrial, or machine-generated information. Data localisation restrictions are imposed by administrative regulations or practices that require particular types of data or datasets to be gathered, processed, and/or kept within a certain geographical region. To put it another way, Member States frequently prefer that data be handled on their own territory.

The European Commission (EC) has recognized such limitations as roadblocks to the free movement of non-personal data throughout the EU, as well as the competitive data economy within the Digital Single Market as a whole. For enterprises, as well as public and governmental institutions, data localisation regulations have become financially and practically burdensome.[88] According to the EC's research, data localisation limitations are particularly troublesome for cloud computing services, because providers frequently use data centres across many states, while outsourced data is regularly transported between these data centres. The use of cloud computing services is discouraged for entities subject to such limitations. To address these concerns, the European Commission, in 2017,

[86] Article 3 (7) LED.
[87] Article 1 (1) LED.
[88] European Commission, EC Communication, Building a European Data Economy, COM(2017) 9, 10.01.2017, available at https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy; EC Staff Working Document on the free flow of data and emerging issues of the European data economy Accompanying the document Communication Building a European data economy, 10.1.2017 SWD(2017) 2 final. Available at https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy.

proposed a legislative instrument, the Regulation on the Free Flow of Non-Personal Data ('Regulation 2018/1807'), with the objective of removing national data localisation limits and this regulation came into effect on May 28, 2019.[89]

Regulation 2018/1807 pertains to non-personal electronic data, which are not subject to the GDPR, and it aims to improve their free movement throughout the EU, in particular by removing national data localisation restrictions on non-personal data kept by a natural or legal person in the EU. When the Member States invoke concerns of public security, an exception is provided. In addition, Regulation 2018/1807 aims to put the idea of data accessibility for regulatory control into practice, which means access to non-personal data kept or processed in the EU would be made easier for competent authorities. Regulation 2018/1807, in Article 5, gives the Member States the option to "*impose effective proportionate and dissuasive penalties for failure to comply with an obligation to provide data, in accordance with Union and national law".*

Self-regulatory solutions, such as the formation of codes of conduct, are also encouraged to facilitate data portability and provider switching, such as cloud service providers. As per Article 6, these codes of conduct should be "*based on the principles of transparency and interoperability and taking due account of open standards, covering, inter alia, the following aspects:*

(a) *Best practices for facilitating the switching of service providers and the porting of data in a structured, commonly used and machine-readable format including open standard formats where required or requested by the service provider receiving the data;*

(b) *Minimum information requirements to ensure that professional users are provided, before a contract for data processing is concluded, with sufficiently detailed, clear and transparent information regarding the processes, technical requirements, timeframes and charges that apply in case a professional user wants to switch to another service provider or port data back to its own IT systems;*

(c) *Approaches to certification schemes that facilitate the comparison of data processing products and services for professional users, taking into account established national or international norms, to facilitate the comparability of those products and services. Such approaches may include, inter alia, quality management, information security management, business continuity management and environmental management;*

[89] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018.

(d) *Communication roadmaps taking a multi-disciplinary approach to raise awareness of the codes of conduct among relevant stakeholders.*"

According to Recitals 33 and 34, any existing (cyber)security rules for storing and processing data will continue to apply if data is stored or processed beyond EU borders or in the cloud.

### 3.4.1. Datasets containing both personal and non-personal information

It is necessary to highlight that most datasets are of mixed nature, which means they contain both personal and non-personal information and, thus, applications of the legal frameworks are not always straightforward. For this reason, The EC has issued guidelines on the relevant framework for mixed datasets and the relationship between Regulation 2018/1807 and the GDPR.[90] By juxtaposing personal and non-personal data, the Guidelines try to explain the scope of the two legal instruments. According to the Guidance, the non-personal data can be classified as data that is initially and by nature non-personal, such as machine-generated data, or data that is turned into non-personal using procedures like anonymization. It is noteworthy that numerous research has questioned the efficacy of anonymization procedures and the extent to which anonymized data should be regarded as non-personal because technology's constant quick evolution frequently allows for their re-identification. For this reason, it is suggested in the literature that anonymised datasets should be given special consideration.[91] Anonymized datasets should not be deemed non-personal data, and in any case, they should be protected from re-identification by strengthened security measures and revision controls.[92]

Thus, determining whether a dataset contains personal data, non-personal data, or is mixed might be difficult. The EC Guidance provides examples of the mixed datasets as follows:

- A company's tax record, mentioning the name and telephone number of the managing director of the company
- Datasets in a bank, particularly those with client information and transaction details, such as payment services (credit and debit cards), Partner Relationship Management (PRM) applications and loan agreements, documents mixing data concerning natural and legal persons

[90] European Commission, Communication, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, COM (2019) 250, 29.05.2019. Available at: https://ec.europa.eu/digital-single-market/en/news/practical-guidance-businesses-how-process-mixed-datasets.

[91] See for example Finck, Michèle, and Frank Pallas. "They Who Must Not Be Identified - Distinguishing Personal from Non-Personal Data Under the GDPR." SSRN Electronic Journal, 2019. Rocher, Luc, Julien M. Hendrickx, and Yves-Alexandre de Montjoye. "Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models." Nature Communications 10, no. 1 (December 2019): 3069.

[92] Daphné Van der Eycken, Ilaria Buri, Plixavra Vogiatzoglou, Anton Vedder, CyberSANE Deliverable D2.2 Legal and Ethical Requirements (2020), p. 45.

- Research institution's anonymised statistical data and the raw data initially collected, such as the replies of individual respondents to statistical survey questions
- Company's knowledge database of IT problems and their solutions based on individual IT incident reports
- Data related to the Internet of Things, where some of the data allow assumptions to be made about identifiable individuals (e.g., , presence at a particular address and usage patterns)
- Analysis of operational log data of manufacturing equipment in the manufacturing industry.

As stipulated under Article 2(2) of Regulation 2018/1807, this regulation should only apply to non-personal data of a mixed dataset, while the GDPR should continue to apply to the mixed dataset's personal data. However, according to the EC Guidance, if the non-personal data and personal data components are "*inextricably linked*," "*the data protection rights and obligations stemming from the GDPR fully apply to the whole mixed dataset, also when personal data represent only a small part of the dataset*", and the condition where data parts are inextricably linked may refer to a situation in which a dataset contains both personal and non-personal data and separating the two would be either impossible or considered by the controller to be economically inefficient or technically impossible. The Guidance further notes that "*neither of the two Regulations obliges businesses to separate the datasets they are controlling or processing. Consequently, a mixed dataset will generally be subject to the obligations of data controllers and processors and respect the rights of data subjects established by the GDPR*."

The Guidance underlines that non-personal data portability is distinct from the right to data portability introduced by the GDPR. Data portability, as defined by Regulation 2018/1807, refers to exchanges between a professional user and a service provider on a business-to-business basis. More precisely, it "*targets a situation where a professional user has outsourced the processing of its data to a third party offering a data processing service".*

In case the PRAETORIAN project uses cloud computing services, the above-explained points should be taken into account, and a provider ensuring data portability should be chosen. If the project processes and stores non-personal data, it must allow for controls by regulatory authorities and must have strong security measures in place. If the project processes mixed datasets, it should make clear to what extent the non-personal data and the personal data parts are inextricably linked and in case this is not possible, the project should adopt separate privacy and confidentiality policies to apply for the non-personal and the personal data.

# 4. The EU legal framework on cybersecurity

This section provides an overview of the EU legal framework on cybersecurity, focusing on some of the most significant initiatives within the EU Cybersecurity strategy: the Directive 2016/1148 on Network and Information Systems (NIS Directive) (including its interconnection with the GDPR),[93] the proposal of the Directive 2020/0359 on measures for a high common level of cybersecurity, across the Union, repealing the Directive 2016/1148 (NIS2 Directive) and the Regulation (EU) 2019/881 on the European Union Agency for Network and Information Security (ENISA) and on information and communications technology cybersecurity certification (Cybersecurity Act).[94] It should be noted that the use cases of the PRAETORIAN project and their specifications are not well defined, yet. This affects the analysis provided in this section, and in many instances different potential scenarios are articulated.

## 4.1. Scope and objectives

Information Communication Technologies (ICT) have become an integral part of most of the critical sectors of the EU economy. Many business models that are followed rely on the high performance and the uninterrupted availability of ICT resources. Such functions can significantly be impacted if they are involved in cybersecurity incidents. Such incidents can have a range of origins including criminal, terrorist and state-sponsored attacks as well as natural disasters and unintentional mistakes. Nevertheless, cybersecurity incidents irrespective of whether they are intentional or unintentional can severely disrupt the normal functioning of critical entities such as ports, airports, power plants and hospitals and the provision of essential services having an immense impact on our society and economy.

In this context, the security of network and information systems has become a core objective of the EU, which over the last decade has significantly intensified its efforts to promote cybersecurity and cyber-resilience at the EU level. The key cybersecurity objectives of the EC is the increase of cybersecurity capabilities and cooperation, the establishment of the EU as a strong player in cybersecurity and embedment of cybersecurity in EU policies.[95]

[93]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 (NIS Directive), OJ L 194, 19.7.2016.
[94]Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, 16.12.2020.
[95]European Commission, EU cybersecurity initiatives, working towards a more secure online environment, 2017.

To achieve these aims the EC launched the first EU Cybersecurity Strategy "An Open, Safe and Secure Cyberspace" in 2013.[96] This includes a comprehensive definition of cybersecurity at EU level as the *"safeguard, and the actions that can be used to protect the cyber-domain, both in the civilian and military fields, from those threats that are associated with or that, may harm its interdependent networks and information infrastructure*".[97] The 2013 Strategy was accompanied by a Proposal for the NIS Directive. This Directive was finally approved in July 2016 and entered into force in August of the same year. The NIS Directive will be further discussed in the section 4.2.

In July 2016, the EC adopted the Communication aiming at "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry".[98] The 2016 Communication included a set of measures aiming at encouraging Member States to use the cooperation mechanisms provided under the NIS Directive and to increase their preparedness for large-scale cyber incidents, supporting the emerging single market for cybersecurity products and services in the EU, and establishing a contractual public-private partnership with industry in order to facilitate cybersecurity industrial capabilities and innovation.

In December 2020, the EC and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy.[99] This strategy was accompanied by a proposal for the reform of the NIS Directive, also known as NIS2 Directive proposal. The 2020 Strategy stipulates that a reformed NIS Directive can provide the basis for more specific rules that are also necessary for strategically important sectors, including energy, transport and health. The NIS2 Directive proposal is further discussed under the paragraph 4.2.3.

In September 2017, the EC adopted a Cybersecurity Package, which encompassed a wide range of measures to enhance cybersecurity, including a proposal for a EU Cybersecurity agency and a EU-wide cybersecurity certification scheme. Such measures and innovations are envisaged in the so-called "Cybersecurity Act", adopted in 2019 and illustrated under the paragraph 4.4.

---

[96]European Commission, High Representative of the EU for Foreign Affairs and Security policy, Joint Communication, Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace, Brussels, 7.2.2013, JOIN (2013).

[97]Alessandro Bruni, Promoting Coherence in the EU Cybersecurity Strategy, in Anton Vedder, Jessica Schroers, Charlotte Ducuing and Peggy Valcke (eds.), Security and Law, Legal and Ethical Aspects of public Security, Cyber Security and Critical Infrastructure Security, Intersentia, 2019.

[98] European Commission, Communication: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, 2016.

[99] European Commission, The EU's Cybersecurity Strategy for the Digital Decade, Shaping Europe's digital future, 2020.

## 4.2. The NIS Directive

This section provides an overview and some key definitions of the NIS Directive. In addition, it continues with the obligations enshrined in the NIS Directive for CIs operators and providers, the interplay between the NIS Directive and the GDPR and the recent NIS Directive proposal. It finally, concludes by providing some insights on the Cybersecurity Act.

### 4.2.1 Overview

The NIS Directive is the first piece of EU legislation on cybersecurity and represents the main output of the "2013 EU Security Strategy".[100] It introduces a set of legal measures aimed at *"achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market*".[101] To achieve this aim the NIS Directive:

- Obliges the Member States to adopt a national strategy on the security of networks and information systems;
- Creates 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;
- Creates a Computer Security Incident Response Teams network (CSIRTs network) to facilitate trust, collaboration and information exchange among Member States;
- Provides security and notification obligations for Operators of Essential Services (OES) and Digital Service Providers (DSP); and
- Obliges Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems.[102]

The NIS Directive introduces a minimum harmonisation in the area of NIS security, allowing for stricter rules to be adopted or maintained at the national level.[103] The obligations of the NIS Directive are addressed at two categories of entities, for which the NIS Directive establishes a different regime: the OES and the DSP.

The PRAETORIAN technology is primarily addressed to CIs which are likely to be identified by the Member States as OES or DSP, and thus they will be subject to the obligations of the NIS Directive.

[100] 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 ("NIS Directive"), OJ L 194, 19.7.2016.
[101] Article 1, NIS Directive.
[102] Ibid.
[103] Article 3, NIS Directive.

PRAETORIAN itself might be considered as a digital service. It is therefore useful to present the main definitions of the NIS Directive and subsequently to describe the main obligations posed by the NIS Directive.

### 4.2.2 NIS Directive's key definitions

NIS Directive defines a **network and information system** as follows:

a) *Electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC86*
b) *Any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data*
c) *Digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance.*[104]

Another key definition provided in the NIS Directive is that of **security of network and information systems**. The latter is defined as "*the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems*".[105]

Moving to the categories of entities towards which the NIS Directive's obligations are addressed, **OES** are defined as "*public or private entities of a type referred to in Annex II*", i.e.,,, energy, transport, banking, financial market infrastructure, health, drinking water supply and digital infrastructure,[106] which abides by the following cumulative criteria set out in Article 5(2) of the NIS Directive, that is:

a) *an entity which provides a **service** which is **essential for the maintenance of critical societal and/or economic activities**;*
b) *the provision of that **service depends on network and information systems**; and*
c) *an incident would have **significant disruptive effects** on the provision of that service.*[107]

[104] Article 4 (1), NIS Directive. It can be noted that the letter b) and c) correspond to the definition of the term information system as set out in the aforementioned Directive 2013/40/EU.
[105] Article 4 (2), NIS Directive.
[106] Annex II, NIS Directive.
[107] Article 5(2), NIS Directive.

For the purposes of the identification of the operators of essential services, each Member State shall establish a list of the services which are essential for the maintenance of critical societal and/or economic activities.[108]

Member States had to identify by 9 November 2018 the operators of essential services established on their territory for each of the sectors and subsectors in Annex II of the NIS Directive, and should update this list at least every two years after 9 May 2018.[109]

However, the NIS Directive does not define the element of "**significant disruptive effect",** which is one of the cumulative criteria set under Article 5(2) of the NIS Directive, but stipulates that what constitutes a significant disruptive effect will be determined on a national level by taking into account the factors listed under Article 6(1) of the NIS Directive, that is:

*(a) The number of users relying on the service;*

*(b) The dependency of other essential services on that service;*

*(c) The possible impact of incidents in regards to the degree and duration on economic and societal activities or public safety;*

*(d) The market share of that entity;*

*(e) The area that could be affected by an incident; and*

*(f) The importance of the entity for maintaining a sufficient level of that essential service, taking into account the availability of alternative means for the provision of that service.*

Moreover, the NIS Directive defines **digital service** as *"any Information society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services'* and *which is either an online marketplace, an online search engine, or a cloud computing service.*[110] Lastly, **DSP** are defined as *'the legal persons which provide a digital service"*.[111]

Lastly, the NIS Directive rules are part of 4 distinct domains:

- Rules on to the governance
- Rules on to the protection (architectures, administration, access control, update, physical sec.)
- Rules on to the defence (detection, incident response)
- Rules on the cyber-resilience of activities

[108] Article 5(4), NIS Directive.
[109] Article 5(1), NIS Directive; Article 5(5) NIS Directive.
[110] Article 4(5), NIS Directive.
[111] Article 4(6), NIS Directive.

### 4.2.3 NIS Directive's obligations

#### 4.2.3.1 National frameworks on the security of network and information systems

Member States must adopt **a national strategy** i.e.,,, a framework providing strategic objectives and priorities on the security of network and information systems at national level.[112] Besides, they shall **designate** one or more **national competent authorities** on the security of network and information systems, covering at least the sectors and the services listed under Annex II and III,[113] and appoint **a national single point of contact** on the security and information systems (which may coincide with the competent authority). The national single point of contact will exercise a liaison function to ensure cross-border cooperation among the authorities of the Member States and also with the Cooperation Group referred to in Article 11 and the CSIRTs' network referred to in Article 12 of the NIS Directive.[114] Finally, Member States have to designate one or more **CSIRTs** that are responsible for risk and incident handling.[115] This national framework is relevant to the OES, as it defines their obligations.

#### 4.2.3.2 Obligations for OES

All the entities that are identified as OES must comply with the **security and incident notification requirements** listed under Article 14 of the NIS Directive.[116]

**A. Security requirements**

To start with the security requirements, OES must adopt **technical and organizational measures** which are appropriate and proportionate to **manage the risks posed to the security of the network and information systems** that they use in their operations.[117] Furthermore, OES must take appropriate measures to **prevent and minimise the impact of incidents on network and information systems used for essential services** in order to ensure the continuity of those services.[118]

The role of the Cooperation Group established under Article 11 of the NIS Directive has been important for the effective and coherent implementation of the NIS Directive across the EU. It has published a series non-binding guidelines to support the Member States in the effective and coherent implementation of the NIS Directive across the EU. More precisely, the first publication of the Cooperation Group (01/2018) addresses the issue of the security measures to be adopted by the

[112] Articles 7 and 4(3), NIS Directive.
[113] Article 8, NIS Directive.
[114] Article 9, NIS Directive.
[115] Articles 8 and 9, NIS Directive.
[116] Article 14, NIS Directive.
[117] Article 14(1), NIS Directive.
[118] Article 14(2), NIS Directive.

OES.[119] Albeit the publication 01/2018 provides non-binding guidelines for the adoption of such measures, it can be a very useful tool that facilitates the compliance of OES.

### B. Incident notification requirements

Moving to the incident notification requirement under the Article 14(3) and (4) of the NIS Directive, the OES have the obligation to **notify the incidents which have a significant impact on the continuity of the essential services that they provide** to the competent authorities or the CSIRTs without undue delay. In the process of assessing the significance of the impact of a security incident and their consequent notification obligations, OES must take into account the following elements provided in Article 14(4) of the NIS Directive, which are:

a) The number of users affected by the disruption of the essential service at hand;
b) The duration of the incident occurred; and
c) The geographical spread of the area concerned by the incident

Additional explanation and guidance on the transposition of the elements of the incident notification provided under the Article 14(3) and (4) of the NIS Directive provides the second publication (02/2018) of the Cooperation Group, "Reference Document on Incident Notification for Operators of Essential Services (Circumstances of Notification)."[120] In this document the Cooperation Group elaborates on the concepts of the number of users affected, the duration of the incident as well as the geographical spread of the incident as follows:

(a) **Number of the users affected** by the disruption of the essential service): the Cooperation Group indicated that in the context of the Article 14(4)(a) of the NIS Directive the number of users affected by the disruption of the essential service at hand means *"the number of affected natural persons and legal entities with whom a contract for the provision of the services has been concluded"*.[121] The way of determining the number of users affected may vary depending on the type of industry and the business models involved. Besides, to properly determine the number of the affected users, OES have to consider both the users of the so-called first layer, i.e.,, those with whom they have direct connection, as

[119] Cooperation Group, Reference document on security measures for Operators of Essential Services, 01/2018. Available at: https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group.
[120] Cooperation Group, Reference Document on Incident Notification for Operators of Essential Services, 02/2018. Available at: https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group.
[121] Ibid.

well as users of the so-called second layer, i.e., the users affected when first layer users provide services based on the particular service that was affected.[122]

(b) **Duration of the incident**: the Cooperation Group identified that in the context of the Article 14(4)(b) of the NIS Directive the duration of an incident is "*the period of time when an essential service offered by a OES is unavailable due to an impairment affecting the confidentiality, integrity, availability or authenticity of the underlying computer system that supports the provision of the service*". The starting point of the incident can be the moment of the identification of the breach, or of the service degradation notice, depending on the incident type at hand. In turn, finalizing the incident might be considered the time where all services have been fully recovered or the time when the systems were fully disinfected (e.g., in case of malware infections). In short, the duration of the incident starts from the moment when the provision of the service was affected until the time of full recovery. What is important is that the parameter of the duration of the incident is interlinked with that of the number of the users affected and should be utmost taken into account.[123]

(c) **Geographical spread** with regard to the area affected by the incident, the Cooperation Group stipulated that in the context of Article 14 (4)(c) of the NIS Directive, the geographical spread of an incident means: "*the Member States or regions within EU where users were affected by impairments of the essential service affected".* The reporting of the geographical spread has to be examined based on the specificities within the different sectors.

Furthermore the Reference Document stipulates that OES are not restricted to the three parameters of Article 14(3).[124] OES can consider additional parameters when assessing the significance of the impact of the incident and evaluating their consequent reporting obligations, such as those for the identification of OES, provided under Article 6 of the NIS Directive. In this context OES can take into consideration:

(d) the **dependency** of other OES sectors on the service provided by the affected entity:[125] for example, a fallout in an energy infrastructure may cause significant disruptions on a variety of other OES, such as those on the transport and health sector.[126] The

[122] Ibid, p.19.
[123] Ibid, p.20.
[124] Ibid, p.8.
[125] Article 6(b), NIS Directive.
[126] Daphné Van der Eycken, Ilaria Buri, Plixavra Vogiatzoglou, Anton Vedder, CyberSANE Deliverable D2.2 Legal and Ethical Requirements (2020), p.51.

interdependencies among OES should be described during the identification process required by Article 5(1) NIS Directive and reported during the notification process. In this context, it is advisable that interdependent OES impose on each other notification obligations and include relevant non-compliance clauses, based on their commercial contracts.

(e) the **impact** that incidents could have**, in terms of degree and duration, on economic and societal activities or public safety**:[127] this parameter is understood as "*the detrimental effects of an incident on the activities of users, that generate either economic or social damages or affect the public safety*".[128]

In the context of the NIS directive, the term of "impact on economic and societal activities" is referred to possible damages brought to the functioning of the EU internal market. This goes beyond the impact on specific OES or on the so-called first-layer users to whom the OES have direct connection/agreement with. The sum of individual impacts suffered by each of the users might be a response in this case, nevertheless these information is unknown to OES.[129]

Besides, the notion of public safety includes the protection of citizens, organizations, and institutions against threats to their well-being – and to the prosperity of their communities. Although in some cases such as in energy or transport, the impact might be known on a relative scale, the real impact can only be measured and communicated by a national authority. Thus, this is also another unknown area for OES.

In this context, it could be supported that this indicator could only be measured properly by governments, national authorities, and other competent bodies and not by the OES. Nevertheless, the indicator of duration is also taken into consideration by the OES, under 14(4)(b) of the NIS Directive as it has been described above.

(f) the **market shares** of that entity: this indicator refers to *"the percentage of a market (defined in terms of either units or revenue) accounted for by a specific entity".* Market share gives a good overview of the importance of an operator on a specific market since

[127] Article 6(c), NIS Directive.
[128] Cooperation Group, Reference Document on Incident Notification for Operators of Essential Services, 02/2018. Available at: https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group, p.22.
[129] Ibid.

knowing the market share might help in identifying possible significant incidents and the extent of their impact. The bigger the market share, the bigger the impact in case of an incident. In more regulated industries such as energy and transport, the market share might be easy to find out, as reporting certain figures regarding their activities is mandatory.

To measure market share it is important to use units of measure that are relevant to the impact that an incident can have. In the context of cybersecurity, taking into account the revenues of a company might not be a suitable option as it will not properly indicate the real impact on the public. In this respect, using other units of measure such as the number of users or the percentage of the total units within a market (e.g., delivered Mega Watts per hour out of total for OES in the domain of energy, passengers or freights transported in the domain of transport, and/or number of patients admitted in a certain hospital in the health domain, etc.) might be a more appropriate option.

(g) the **geographic spread** with regard to the area that could be affected by an incident: this parameter is identical to the geographical spread explained under Article 14 (4)(c) of the NIS Directive.[130]

(h) the **importance of the entity** for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service:[131] this indicator looks at the availability of alternative means for the provision of the service, which may come from inside the OES, (e.g., , the use of another means of transport or another energy supplier, etc.), or from outside, by using another OES. When alternative means are available for the provision of the service, especially within the same OES, the incident might not reach the threshold of "significance". On the other hand, the lack of alternative means to provide the service turns most of the incidents into significant, especially in cases where the service is of basic need for the population.

In terms of the **notification timeline**, the NIS Directive provides under Article 14(3) that *"Member States shall ensure that operators of essential services notify, without undue delay*".[132] The meaning of "undue delay" might be as soon as the operator is aware of the significant incident, as soon as the

[130] See comment under 4.3.2.2 (c).
[131] (Article 6(f)), NIS Directive.
[132] Article 14(3), NIS Directive.

triggering event occurs (e.g., a cyber-incident leaving 1 million people without energy might be the trigger for the notification, even though not all details are known soon after the blackout).[133] In most of the Member States there are two or three phases of reporting i.e.,, a preliminary reporting, an intermediate reporting and a full reporting.

| CASE | REQUIREMENT |
|---|---|
| A PRAETORIAN end-user qualifies as OES under the NIS Directive. | The technical partners developing the PRAETORIAN technology must consider that the end-users must adopt technical and organizational measures appropriate to manage the risks posed to the security of their network and information systems, as required under the NIS Directive.<br><br>The PRAETORIAN technology must enable the prompt detection of an incident having a significant impact on the continuity of the essential service, as the OES end-users are subject to a duty to notify such incident without undue delay. |

#### 4.2.3.3 Obligations for DSP

Unlike with the OES, the NIS Directive does not require the identification of DSP by Member States. Thus, all the entities which fall into the definition of DSP, are governed by the legal framework of the NIS Directive. DSP can be online market place providers, online search engine providers and cloud service providers.[134]

Alike to the OES, all the entities who are DSP have **security and incident notification obligations**, as provided under the **Article 16 of the NIS Directive.**[135]

**A. Security requirements**

[133] Cooperation Group, Reference Document on Incident Notification for Operators of Essential Services, 02/2018. Available at: https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group, p.9.
[134] Annex III, NIS Directive.
[135] Article 16, NIS Directive.

To start with the security requirements, DSP must adopt technical and organizational measures which are appropriate and proportionate to manage the risks posed to the security of the network and information systems that they use in their operations.[136] The measures adopted shall ensure a level of security of network and information systems that is appropriate to the risk posed. With this aim the **security measures** have to be adopted with due consideration of the following elements:

(a) the security of systems and facilities;
(b) the incident handling;
(c) the business continuity management;
(d) the monitoring, auditing and testing; and
(e) the compliance with international standards.

At the same time DSP shall take appropriate measures to prevent and minimise the impact of incidents on network and information systems used in their operations to ensure the continuity of those services.

### B. Incident notification requirements

Moving to the incident notification obligation, the Article 16(3) of the NIS Directive requires that **DSP shall notify the competent authority or the CSIRT** of any **incident that has a substantial impact** on the provision of a service that they provide in their operations within the EU, **without undue delay**.[137] These notifications must include information with the aim to enable the competent authority or the CSIRT to determine the significance of any cross-border impact. It is good to clarify that the notification of an incident does not make the notifying party subject to increased liability.

Similarly, with the OES regime, DSP in order to determine whether the impact of an incident is **substantial** and their consequent notification obligation, have to take into account the following parameters:

(a) the number of users affected by the incident, in particular users relying on the service for the provision of their own services;
(b) the duration of the incident;
(c) the geographical spread with regard to the area affected by the incident;
(d) the extent of the disruption of the functioning of the service and

[136] Article 16(1) NIS Directive.
[137] Article 16(3), NIS Directive.

(e) the extent of the impact on economic and societal activities.

What is important is that this notification obligation of DSP is not absolute. The DSP are obliged to notify an incident **only when they have access to the information needed to assess the impact of an incident** against the parameters referred under (a) to (e).[138] Such notification must also include **information regarding the** possible **impact** that the incident occurred in the course of the DSP operations, could have **on the provision of an essential service**.[139] This obligation could be of relevance in the course of PRAETORIAN, in case that a PRAETORIAN end-user who qualifies as an OES relies on the provision of services of an DSP e.g., a cloud service provider.

The elements that have to be considered for the adoption of security measures, as well as the elements that must be taken into consideration to determine the significance of the incident are further specified in the Commission Implementing Regulation 2018/152 of 30 January 2018.[140]

In that respect, it is provided that the notion of **security of systems and facilities** means *"the security of network and information systems and of their physical environment"*.[141] Such security shall include, the systematic management of network and information systems, their physical and environmental security, the security of supplies as well as the access controls to network and information systems.

Moreover, the Commission Implementing Regulation 2018/151 of 30 January 2018 provides a list of the **elements that the measures adopted by the DSP shall include**, which are: the detection processes and procedures maintained and tested to ensure timely and adequate awareness of anomalous events; the processes and the policies on reporting incidents and identifying weaknesses and vulnerabilities in their information systems; a response in accordance with established procedures and reporting the results of the measures taken; and an assessment of the incident's severity, documenting knowledge from incident analysis and collection of relevant information which may serve as evidence and support a continuous improvement process.[142]

---

[138] Article 16(4), NIS Directive.
[139] Article 16(5), NIS Directive.
[140] Article 2, Commission Implementing Regulation (EU) 2018/151- of January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be considered by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact, OJ L 26/48, 31.01.2018.
[141] Ibid.
[142] For more details see: Commission Implementing Regulation (EU) 2018/151- of January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact ("Commission Implementing Regulation 2018/151"), OJ L 26/48, 31.01.2018.

The Commission Implementing Regulation 2018/152 of 30 January 2018, also specifies the **parameters that have to be considered to determine the severity of an impact**.[143] In this context the parameters listed in Article 16(4) of the NIS Directive are further specified. Namely:

With regard to **the number of users affected by the incident,**[144] in particular users relying on the service for the provision of their own services, the DSP shall be in a position to estimate either the number of the affected natural and legal persons with whom a contract for the provision of the service has been concluded or the number of affected users having used the service based in particular on previous traffic data.[145]

Moreover, it is specified that the term **duration of the incident,**[146] refers to the time period from the disruption of the proper provision of the service in terms of availability, authenticity, integrity or confidentiality until the time of recovery.[147] As far as the **geographical spread** with regard to the area affected by the incident ,[148] it is clarified that the DSP shall be in a position to identify whether the incident affects the provision of its services in specific Member States.[149] Besides, the extent of the **disruption of the functioning of the service** shall be measured as regards to the availability, authenticity, integrity or confidentiality of data or related services.[150] With regard to the **extent of the impact** on economic and societal activities,[151] the DSP shall be able to conclude, based on indications such as the nature of their contractual relations with the customer or, where appropriate, the potential number of affected users, whether the incident has caused significant material or non-material losses for the users such as in relation to health, safety or damage to property.[152]

Lastly, the Commission Implementing Regulation 2018/152 of 30 January 2018, provides that an incident shall be considered as having a **substantial impact** where at least one of the following situations has taken place. Namely when:

- the service provided by a DSP was unavailable for more than 5.000.000 user-hours;[153]
- the incident has resulted in a loss of integrity, authenticity or confidentiality of stored, transmitted or processed data or the related services offered by, or accessible via a

[143] Article 3, Commission Implementing Regulation 2018/151.
[144] 16(4)(a), NIS Directive.
[145] Article 3(1), Commission Implementing regulation 2018/151.
[146] 16(4)(b), NIS Directive.
[147] Article 3(2), Commission Implementing regulation 2018/151.
[148] 16(4)(c) NIS Directive.
[149] Article 3(3), Commission Implementing regulation 2018/151.
[150] 16(4)(d) NIS Directive; Article 3(4), Commission Implementing regulation 2018/151.
[151] 16(4)(e) NIS Directive.
[152] Article 3(5), Commission Implementing regulation 2018/151.
[153] The term user-hour refers to the number of affected users in the Union for a duration of 60 minutes.

network and information system of the DSP and has affected more than 100.000 users in the EU;

- the incident has created a risk to public safety, public security or of loss of life; or
- the incident has caused material damage to at least one user in the Union where the damage caused to that user exceeds 1.000.000 Euros.

| CASE | REQUIREMENT |
|---|---|
| In case a PRAETORIAN provider qualifies as DSP under the NIS Directive. | The development of PRAETORIAN technology must consider the obligations to which a PRAETORIAN DSP will be subject under the NIS Directive (Article 16), concerning security and notification obligations. The notification of an incident with substantial impact on the provision of a PRAETORIAN cloud service must refer to the possible impact on the provision of an essential service by an OES. |

## 4.3 The interplay between the NIS Directive and the GDPR

While the release of the NIS Directive and the GDPR largely coincided,[154] neither of the two legal instruments acknowledges each other in their texts.[155] The focus of the NIS Directive and the GDPR is different, nevertheless the two legal frameworks are interrelated in some aspects.[156]

The NIS Directive aims at ensuring the cybersecurity of information and communication systems, while the GDPR aims at the protection of personal data. However, when personal data is processed though network and information systems, the two legal frameworks apply at the same time. It is good to be

[154] The NIS Directive was published in July 2016 and the GDPR in April of the same year.
[155] The NIS Directive refers only to the Data Protection Directive (Directive 95/46) that the GDPR replaced, in its Article 2. Nevertheless, at the time when the NIS Directive published, the GDPR had been already published. Besides, the only reference to the Data Protection Directive is the following: "processing of personal data pursuant to this Directive shall be carried out in accordance with Directive 95/46/EC".
[156] Dimitra Markopoulou, Vagelis Papakonstantinou, Paul de Hert, The EU Cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, Computer Law and Security Law Review 35 (2019).

noted that both the NIS Directive and the GDPR impose requirements on operators to adopt risk-based measures.[157] At the same time, both legal frameworks impose incident notification obligations. [158]

The GDPR requires breach notification only where personal data is at stake and thus the competent data protection supervisory authority shall be informed without undue delay and, where feasible, not later than 72 hours after having come aware of the incident. In turn, the NIS Directive mandates breach notification if there is a significant disruption to the provision of the specific service, without undue delay.

Nevertheless, the obligations enshrined by each of the legal instruments have different objectives, and compliance with these obligations should be evaluated separately, for distinct purposes, and by different authorities.[159] In this context, it is important to address compliance with the obligations of each legal instrument, separately.[160] Thus, the adopted security measures should be listed in the NIS Directive and the GDPR compliance documentations, separately. Besides, in case an incident falls under both the legal frameworks, providers, have to notify both the competent authority under the NIS Directive and the respective Data Protection Authority under the GDPR. Such an incident could potentially lead to two distinct fines under the NIS Directive on the one hand and the GDPR on the other.

In case of conflict between the provisions of the NIS Directive and the GDPR, it has to be sorted out on the basis of the *lex specialis/lex generalis* doctrine. The GDPR implementing the fundamental right to data protection is *lex specialis* and will have to prevail over the more general objectives pursued through the cybersecurity initiatives. [161] Besides, potential conflict might arise between the GDPR and the Member State laws which implement the NIS Directive. An example of such a potential conflict could arise when a certain type of processing activities which is prohibited or subject to strict safeguards under the GDPR, is allowed by a certain Member State law implementing the NIS Directive.[162] In that case, normally, the GDPR, as a regulation would prevail over the national legislation implementing the NIS Directive.[163]

[157] Articles 14(1), 16(1) and 17, NIS Directive; Article 25 and 31, GDPR.
[158] Articles 14(3) and 16(3), NIS Directive; Article 33(1), GDPR.
[159] ibid, p.10.
[160] ibid.
[161] ibid, p.11.
[162] ibid.
[163] Preamble para. 75, NIS Directive.

| CASE | REQUIREMENT |
|---|---|
| A PRAETORIAN end-user is subject to the obligations of the NIS Directive and when processing personal data, they are simultaneously subject to the GDPR. | GDPR and NIS Directive obligations apply simultaneously. Operators should address the compliance requirements enshrined in each framework, separately, for example by keeping two separate lists of the measures taken to comply with the obligations under the NIS Directive and the GDPR, respectively. |

## 4.4 The NIS2 Directive proposal

The NIS2 Directive proposal aims at addressing the deficiencies of the NIS Directive, to adapt it to the current needs and to make it future-proof. To this aim, it modernizes the existing legal framework taking account of the increased digitization of the internal market in recent years and the evolving cybersecurity threat landscape. In this context, it introduces measures related to cybersecurity and obliges Member States to adopt a national strategy for the security of networks and information systems.[164]

The NIS2 Directive proposal provides for a **more comprehensive coverage of sectors and services**, compared to the Nis Directive. In addition to the sectors already covered under the NIS Directive, i.e.,, energy, transport, banking and financial market infrastructure, health, drinking water, digital infrastructure and certain digital service providers, the NIS2 Directive proposal adds new sectors, i.e.,, telecoms, chemicals, food, postal and courier services, certain manufacturing, public administration, social-networking platforms, space, waste management and wastewater management.[165]

One of the core changes enshrined in the NIS2 Directive proposal is that **instead of the current identification of individual operators at a national level, the proposed rules introduce a size-cap** to cover, within the selected sectors, all medium and large enterprises as defined under EU law.[166] Moreover, the NIS2 Directive proposal no longer distinguishes between OES and DSP but, instead, classifies **entities as essential or important.**[167] Besides, it broadens the **extra-territorial effect** which is

[164] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, 16.12.2020.
[165] Annex II, NIS2 Directive.
[166] Preamble para 8 and Article 2, NIS2 Directive.
[167] Explanatory memorandum, section 5; preamble para 7; Articles 1 and 2; Annexes I and II, NIS2 Directive.

in place under the current regime, i.e.,, selected providers of digital infrastructure or digital services who do not have an establishment within the EU, but offer services in the EU, will also fall under the scope of the NIS2 Directive proposal.[168] Last, the NIS2 Directive provides for **higher penalties** compared to the NIS Directive, and in that context, EU Member States would be required to provide for administrative fines up to at least 10 million Euros or 2% of the total worldwide turnover.[169]

It is worth noting that NIS2 at this moment is not applicable to the PRAETORIAN tools and it developments or research activities. However, in a case if NIS2 will be into force in the future, it will give the PRAETORIAN products some benefit in advance concerning the Incident Response and Detection systems.

## 4.5 The Cybersecurity Act

Another important EU legal framework aiming to achieve a high level of cybersecurity, cyber resilience and trust within the EU is the Cybersecurity Act.[170] The Cybersecurity Act was adopted on 12 March 2019 and entered into force on 27 June of the same year. While the NIS Directive applies only to OES and DSP, the Cybersecurity Act encourages all businesses to invest more in cybersecurity in order to raise the trust of consumers and industry players in the cyber-resilience of ICT solutions.

In a nutshell, the Cybersecurity Act:

- **Strengthens ENISA** by granting to the agency a permanent mandate, defining its objectives, tasks and organisation (management and operation) and reinforcing its financial and human resources and overall enhancing its role in supporting the EU to achieve a common and high-level cybersecurity.
- Besides, it establishes the first **EU-wide cybersecurity certification framework** to ensure a common cybersecurity certification approach in the European internal market and ultimately to improve cybersecurity in a broad range of ICT products, services and processes.

[168] Preamble para. 64 and Article 24, NIS2 Directive.
[169] Article 31, NIS2 Directive.
[170] 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"), OJ L 151/15, 7.6.2019.

The **first part of the Cybersecurity Act**, focus on redefining and expanding the role of ENISA.[171] It mandates ENISA to contribute to the development, implementation and review of the EU cybersecurity policy and legislation through a variety of actions, including by:

**a)** providing its independent opinion and analysis;

**b)** assisting Member States in the consistent implementation of EU policy and law on cybersecurity, and in particular with regard to the NIS Directive;

**c)** assisting Member states and EU institutions, bodies, offices and agencies in developing and promoting cybersecurity policies related to the availability or integrity of the public core of the open internet;

**d)** contributing to the work of the Cooperation Group provided under Article 11 of the NIS Directive;

**e)** supporting the development of EU policies in the field of electronic identity and trust services, the promotion of electronic communications security and the national implementation of specific cybersecurity aspects of Union policy and law relating to data protection and privacy; and by

**f)** preparing an annual report on the state of the implementation of the legal frameworks regarding incident notification.[172]

Furthermore, the Cybersecurity Act grants ENISA an important role in a range of key areas, such as:

**a)** **Capacity-building** towards Member States, EU institutions, the Cooperation Group and the CSIRTs provided in NIS Directive;[173]

**b)** **Operationa**l **cooperation at the EU level**, among Member States, Union institutions, bodies, offices and agencies, and between stakeholders;[174]

**c)** **Promotion** of the development and implementation of EU policy on **cybersecurity certifications** of and establishment and take-up of European and international **standards** for the security ICT products, services and processes, as well as close monitoring and analysis of the main trends in the **cybersecurity market** on both the demand and supply sides;[175]

[171] Articles 3-45, Cybersecurity Act.
[172] Article 5, Cybersecurity Act.
[173] Article 6, Cybersecurity Act.
[174] Article 7, Cybersecurity Act.
[175] Article 8, Cybersecurity Act.

**d) Knowledge and information**;[176]

**e) Awareness-raising and education**;[177]

**f) Research and innovation**;[178]

**g) International cooperation;**[179]

It can be noticed that a range of the Cybersecurity Act's provisions further support or advance the provisions and the implementation of the NIS Directive.

The **second part of the Cybersecurity Act** lays down the first EU-wide cybersecurity certification framework aiming to create a digital single market for ICT products, services and processes.[180] The certification scheme aims at attesting that the certain products, services and processes, which must be duly identified in the EU work rolling programme, comply with specified security requirements aiming to protect the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, these ICT products, services and processes throughout their life cycle.[181]

The **ENISA develops draft cybersecurity certification schemes**, upon request of the EC or the EU Member States.[182] In the preparation of such schemes, ENISA is supported by a group of experts and collaborates closely with the EC, EU countries, and relevant stakeholders.[183]

The security **objectives** pursued by the certification scheme include: the protection of the data stored, transmitted or otherwise processed, against accidental or unauthorised storage, processing, access, disclosure, destruction, loss, alteration or lack of availability; the access to data, services or functions only by authorized persons; the identification of known dependencies and vulnerabilities; the monitoring of the access, use or otherwise processing of data, services or functions; the restoration of the availability and access to data, services and functions in a timely manner; the security by default and by design; the provision of ICT products, services and processes with up-to-date software and hardware.[184]

[176] Article 9, Cybersecurity Act.
[177] Article 10, Cybersecurity Act.
[178] Article 11, Cybersecurity Act.
[179] Article 12, Cybersecurity Act.
[180] Articles 46-65, Cybersecurity Act.
[181] Article 46(2), Cybersecurity Act.
[182] Article 48, Cybersecurity Act.
[183] Article 49(3)(4)(5)(6), Cybersecurity Act.
[184] Article 51, Cybersecurity Act.

An EU cybersecurity certification scheme may specify one or more **assurance levels** for ICT products, services and processes, ranging from "basic", to "substantial" or "high", depending on the level of the risk associated with the intended use of that ICT product, service or process, in terms of the probability and impact of an incident.[185] Besides, for ICT products, services and processes which present a low risk corresponding to assurance level "basic", an EU cybersecurity certification scheme may allow for the **conformity self-assessment** under the sole responsibility of the manufacturer or the provider of such products, services or processes.[186]

An EU cybersecurity certification mechanism will include **at least the elements** detailed under the Article 54 of the Cybersecurity Act, which are among others, the subject matter and the scope of the certification scheme; a clear purpose of the scheme and of the operativity of selected standards (including international, European or national), evaluation methods, technical specifications and assurance levels; reference to the possibility of conformity self-assessment; specific evaluation criteria; possible marks and labels and specific or additional requirements; rules for monitoring compliance with the requirements of European cybersecurity certificates or the EU statements of conformity; the conditions for issuing, maintaining, continuing and reviewing the EU cybersecurity certificates, etc.[187]

Moreover, the manufacturer or provider of certified ICT products, services and processes must make available the **supplementary cybersecurity information**, i.e.,[188] to provide guidance and recommendations, in order to indicate the period during which assistance is guaranteed, their contact information and a reference to online repositories reporting publicly disclosed vulnerabilities. This information shall be available in electronic form, accessible and updated at least until the expiry of the respective EU cybersecurity certification scheme.[189]

In the context of an EU cybersecurity certification scheme, the Cybersecurity Act prescribes that Member States shall designate one or more **national cybersecurity certification authorities**, which will perform a range of tasks including:

- The supervision and enforcement of the rules included in the EU cybersecurity certification schemes to monitor the compliance of ICT products, services and processes (and of their manufacturers and providers) with the requirements set out under such schemes;

[185] Article 52, Cybersecurity Act.
[186] Article 53, Cybersecurity Act.
[187] For the full list of the elements of the European cybersecurity certification schemes see also: Article 54, Cybersecurity Act.
[188] Article 55, Cybersecurity Act
[189] Article 55(2), Cybersecurity Act.

- The provision of support the national accreditation bodies in monitoring the conformity assessment bodies; and
- The annual reporting of their activities to ENISA and the European Cybersecurity Certification Group (ECCG) established under the Article 62 of the Cybersecurity Act.[190]

Besides, the Cybersecurity Act establishes **assessment bodies** to determine conformity with the Cybersecurity Act and the ECCG, which aims to assist the EC and ENISA.[191] Besides, it requires Member States to determine penalties for certification violations and infringement of EU cybersecurity certification schemes.[192] Unless otherwise provided by EU or Member State law, the cybersecurity certification is voluntary.[193]

Each EU cybersecurity certification scheme will attest that the certified products and services comply with specific requirements. [194] In particular it should specify:

- the categories of products and services covered;
- the cybersecurity requirements, such as standards or technical specifications;
- the type of evaluation, such as self-assessment or third party and
- the intended level of assurance

In July 2019, the EC requested ENISA to prepare a candidate European cybersecurity certification scheme in accordance with the Article 48(2) of the Cybersecurity Act.[195]

Following that request, ENISA set up an Ad Hoc Working Group to support the preparation of a candidate EU cybersecurity certification scheme as a successor to the existing schemes operating under the Senior Officials Group Information Systems Security Mutual Recognition Agreement (SOG-IS MRA). This has been named as EUCC (Common Criteria based European candidate cybersecurity certification scheme) and is the foundation of an EU cybersecurity certification framework. EUCC looks into the certification of ICT products cybersecurity, based on the Common Criteria, the Common

[190] Article 58, Cybersecurity Act.
[191] Articles 60 and 62, Cybersecurity Act.
[192] Article 65, Cybersecurity Act.
[193] Article 56, Cybersecurity Act.
[194] European Commission, The EU cybersecurity certification framework, Shaping Europe's framework, 2022. Available at: The EU cybersecurity certification framework | Shaping Europe's digital future (europa.eu). Accessed on May 18, 2022
[195] ENISA, Crossing a bridge: the first EU cybersecurity certification scheme is availed to the Commission, 2021. Available at: Crossing a bridge: the first EU cybersecurity certification scheme is availed to the Commission — ENISA (europa.eu).

Methodology for Information Technology Security Evaluation, and the corresponding standards, respectively, ISO/IEC 15408 and ISO/IEC 18045.[196]

In accordance with Article 49(3) of the Cybersecurity Act, ENISA launched a public consultation from July, 2 to July, 31 2020 after developing a draft candidate EUCC.[197] The outcome of the public consultation confirmed the intent of certification stakeholders to use the scheme in the internal market, when it will be available. Besides, it showed that stakeholders encourage ENISA to further develop guidance to support the implementation and execution of the scheme and they indicated some elements that needed to be adjusted or fixed. As a result, some significant changes were implemented to the draft candidate EUCC, including the addition and clarification of definitions.[198]

ENISA has currently submitted the candidate EUCC scheme to the EC in line with the provisions of Article 49 (6) (7) of the Cybersecurity Act.[199] The EC will initiate a Commission Implementing Regulation that may be adopted.

| **CASE** | **REQUIREMENT** |
|---|---|
| PRAETORIAN-related products, services or processes will ultimately be offered on the market. | The PRAETORIAN partners who are involved in the development of the products, services or processes at hand, as well as the producers or manufacturers must monitor the rules related to the EUCC scheme and the progress towards their adoption, in order to be able to comply with such rules and ultimately to receive such certification when available. |

[196] ENISA, Cybersecurity Certification: Candidate EUCC Scheme, 2020. Available at: Cybersecurity Certification: Candidate EUCC Scheme — ENISA (europa.eu).
[197] Report on Public consultation on the draft candidate EU Scheme, 2021. Available at: Cybersecurity Certification: Candidate EUCC Scheme V1.1.1 — ENISA (europa.eu).
[198] According to the Report, it introduced the clarification of activities related to the maintenance of certificates and of deadlines associated to the handling of non-conformities, non-compliances and vulnerabilities, including the modification of the status of the new patch management process and of the logo associated to the certificates, the clarification of the peer assessment requirements and simplification of the associated annex, etc. See Report on Public consultation on the draft candidate EU Scheme, 2021. Available at: Cybersecurity Certification: Candidate EUCC Scheme V1.1.1 — ENISA (europa.eu)
[199] ENISA, Cybersecurity Certification, EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS, V.1.1.1, May 2021. Available at: Cybersecurity Certification: Candidate EUCC Scheme V1.1.1 — ENISA (europa.eu).

# 5. Critical Infrastructures in the EU

## 5.1. The protection of Critical Infrastructures

This section is aimed at providing a general overview of the EU legal framework concerning the protection of CI, which is relevant to the PRAETORIAN in light of its focus on the protection of CI. In this context, this section elaborates on the notion of critical infrastructures, the rules of the Directive 2018/114/EC on the protection of European Critical Infrastructures (ECI Directive) that govern the CIs protection,[200] as well as the proposal for a Directive on the resilience of critical entities (also known as 'CER Directive proposal'), which aims at replacing the ECI Directive.[201]

## 5.2. The ECI Directive

Following the communication from the EC to the Council and the European Parliament of October 2004 regarding the CIs Protection in the fight against terrorism, the EU adopted the ECI Directive in December 2008. To date, the ECI Directive is the most important legal framework in relation to the physical protection of the CIs in the EU. This Directive establishes "*a procedure for the identification and designation of ECIs, and a common approach to the assessment of the need to improve the protection of such infrastructures in order to contribute to the protection of people*".[202]

### 5.2.1 The notions of Critical Infrastructures and European Critical Infrastructures

The ECI Directive provides the fundamental definitions of the notions of CIs and ECI. More concretely, it defines the notion of **CIs** as "*an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.*"[203]

Besides, it defines the notion of **ECI** as *'[a] critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States (*emphasis added). *The significance of the impact shall be assessed in terms of cross-cutting criteria, including the effects resulting from cross-sector dependencies on other types of infrastructure'*.[204]

[200] 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 OJ L 345/75 23.12.2008 (ECI Directive).
[201] Directive 2020/0365 on the resilience of critical entities (CER Directive), 16.12.2020.
[202] Article 1, ECI Directive.
[203] Article 2(a), ECI Directive.
[204] Article 2(b), ECI Directive.

It is important to note that the ECI Directive's scope is on the protection of ECI, and thus the identification and protection of national CIs that only affects one Member State remain outside of its scope. Besides, the ECI Directive, adopts a sectoral approach by establishing a procedure for identifying and designating ECI in the energy (i.e.,, electricity, oil and gas) and transport (i.e.,, road, rail, air, inland waterways transport, as well as ocean and short-sea shipping and ports) sectors.[205] It aims on enhancing the security of physical assets against threats such as terrorism and other intentional and unintentional man-made threats, as well as natural disasters.

### 5.2.2 The rules of the ECI Directive

The Article 3 of the ECI Directive, requires each Member State to identify the CI which may be designated as an ECI. To that aim, each Member State shall follow a series of consecutive steps.[206] The procedure for the Identification of CI which may be designated as an ECI is described in detail in the Annex III of the ECI Directive.[207]

A potential ECI which does not satisfy the requirements of one of the following sequential steps, does not move to the next step, is considered to be 'non-ECI' and is excluded from the procedure. The steps that should be followed for the designation of a CI as ECI are the following:

> **Step 1**- *Each Member State shall apply the sectoral criteria in order to make a first selection of critical infrastructures within a sector.*
>
> **Step 2**- *Each Member State shall apply the definition of critical infrastructure pursuant to Article 2(a) to the potential ECI identified under Step 1.*
>
> *The significance of the impact will be determined either by using national methods for identifying CIs or with reference to the cross-cutting criteria, at an appropriate national level. For infrastructure providing an essential service, the availability of alternatives, and the duration of disruption/recovery will be taken into account.*
>
> **Step 3** - *Each Member State shall apply the transboundary element of the definition of ECI pursuant to Article 2(b) to the potential ECI that has passed the first two steps of this procedure. A potential ECI which does satisfy the definition will follow the next step of the procedure. For infrastructures providing an essential service, the availability of alternatives, and the duration of disruption/recovery will be taken into account.*

[205] Annex II, ECI Directive.
[206] Annex III, ECI Directive.
[207] ibid.

> **Step 4** - *Each Member State shall apply the cross-cutting criteria to the remaining potential ECI. The cross-cutting criteria shall take into account: the severity of impact; and, for infrastructure providing an essential service, the availability of alternatives; and the duration of disruption/recovery. A potential ECI which does not satisfy the cross-cutting criteria will not be considered to be an ECI.*

A potential ECI which has passed through all the steps of this procedure shall only be communicated to the Member States which may be significantly affected by the potential ECI.

Moving to the **obligations of ECI operators**, the ECI Directive mandates them to have in place an **Operator Security Plan (OSP) or equivalent measures** with the aim to identify critical infrastructure assets as well as existing security solutions.[208] An ECI OSP procedure should cover at least the identification of important assets, a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact, and the identification, selection and prioritisation of counter-measures and procedures with a distinction between permanent and graduated security measures.[209] The OSP or the equivalent measures should be reviewed regularly within one year following the designation of the critical infrastructure as a ECI. [210] In addition, each ECI operator must appoint a **Security Liaison Officer** responsible to serve as a point of contact regarding security-related issues between the ECI operators and the Member State authorities.[211]

On the Member States' side, they must implement **appropriate communication mechanisms** aiming to facilitate the information exchange concerning identified risks and threats in relation to the ECI concerned, between the relevant Member State authorities and the Security Liaison Officers.[212] Moreover, the ECI Directive includes provisions regarding ECI-related **information handling and reporting requirements**, including the obligation for each Member State to conduct 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, etc.[213]

The ECI Directive constitutes an important first step towards the protection of ECI. Nevertheless, it does not provide for substantive measures for the protection of ECI, and the primary and ultimate responsibility for protecting ECI falls on the Member States and the owners/operators of such

[208] Article 5, ECI Directive.
[209] Annex II, ECI Directive.
[210] Article 5(3), ECI Directive.
[211] Article 6(1), ECI Directive.
[212] Article 6(4), ECI Directive.
[213] Article 7, ECI Directive.

infrastructures.[214] Nevertheless, the ECI Directive includes only general rules regarding the appointment of the ECI protection contact points,[215] and the handling of written **ECI-related classified information**. The only substantial requirement that it sets in that respect is that Member States, the EC and relevant supervisory bodies have to ensure that sensitive ECI protection-related information is not used for any purpose other than the protection of ECI, whereas it leaves under the competence of each Member State to regulate these aspects.

In light of the constantly changing cybersecurity threat landscape, in August 2018 the EC launched an evaluation of the ECI Directive to analyse its implementation and application in each EU Member State according to a number of specific criteria set out in the Commission's Better Regulation Guidelines, and namely relevance, coherence, effectiveness, efficiency, EU added value and sustainability.[216] The evaluation analysed the scope and content of the ECI Directive, the organisation of work at the national and EU level aimed at implementing the ECI Directive, and the state of implementation of the ECI Directive's provisions. The purpose of the impact assessment was to provide the EC with a qualitative and quantitative analysis of the ECI Directive and with recommendations as to how to further strengthen the protection and resilience of the ECI, and to explore different policy options to address the challenges that the recent technological, economic, social, policy/political and environmental developments impose for the ECI protection.

The above evaluation as well as the impact assessment, accompanying the proposal for the CER Directive,[217] showed that existing European and national measures face limitations in helping operators to confront the operational challenges that they face today and the vulnerabilities that their interdependent nature entail. To address these problems, four options were stipulated.

The Option number 1 advocated for the adoption of non-legislative measures at the EU level aiming to encourage more common approaches and information sharing. The Option number 2 entailed the development of revised criteria and requirements for operators of ECI. The Option number 3 supported the development of new requirements for critical entities with the replacement of the ECI Directive with a new instrument. Last, the Option number 4, stipulated the replacement of the ECI

[214] Preamble para. 6, ECI Directive.
[215] Article 10, ECI Directive.
[216] European Commission, Commission Staff Working Document, Evaluation of Council Directive 2008/114 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve protection, 23.07.2019. Available at: 20190723_swd-2019-308-commission-staff-working-document_en.pdf (europa.eu).
[217] European Commission, Commission staff working document Impact assessment, accompanying the document for the proposal for a Directive of the European parliament and of the Council on the resilience of critical entities, 16.12.2020. Available at: impact_assessment_swd-2020-358.pdf (europa.eu).

Directive with a new instrument, while at the same time reinforcing the role of the EU by establishing a more substantial role for the EC in identifying critical entities and the creation of a dedicated EU Agency responsible for critical infrastructure resilience.[218]

The impact assessment found that the preferred option was the replacement of the ECI Directive with a new instrument aimed at enhancing the resilience of critical entities in the sectors considered as essential by the NIS2 Directive proposal, and proceeded with the CER Directive proposal.[219]

## 5.3 The CER Directive proposal

In order to ensure a consistent approach for the protection of CIs both against cyber and physical threats and in line with the Security Union Strategy 2020-2025, the NIS2 Directive proposal was proposed together with the CER Directive proposal.

The CER Directive proposal reflects the priorities of the EC's EU Security Union Strategy for a revised approach to CIs resilience that better reflects the current and anticipated future risk landscape, the increasingly tight interdependencies between different sectors and the increasingly interdependent relationships between physical and digital infrastructures.

The CER Directive proposal will have a much wider sectoral scope that the ECI Directive. While ECI Directive covers only the sectors of energy and transport, the CER Directive proposal covers also the sectors of banking, financial market infrastructure, health, drinking water, waste water, digital infrastructures, public administration and space.[220]

Moving to the core elements of the CER Directive proposal, it provides for a procedure for EU countries to identify critical entities based on a national risk assessment. At the same time, it lays down obligations for Member States to take certain measures aimed at ensuring the provision in the internal market of services essential for the maintenance of vital societal functions or economic activities and in particular to identify critical entities and entities to be treated as equivalent in certain respects, and to enable them to meet their obligations. Besides, it establishes obligations for critical entities aimed at enhancing their resilience and improving their ability to provide those services in the internal market

[218] For more information see Explanatory memorandum, section 3, CER Directive.
[219] European Commission, Commission staff working document Impact assessment, accompanying the document for the proposal for a Directive of the European parliament and of the Council on the resilience of critical entities, 16.12.2020. Available at: impact_assessment_swd-2020-358.pdf (europa.eu); Explanatory memorandum, section 3, CER Directive.
[220] Annex, CER Directive.

as well as rules on supervision and enforcement of critical entities, and specific oversight of critical entities considered to be of particular European significance.

## 5.4 ECI Directive vs NIS Directive

Both the NIS and the ECI Directives aimed at ensuring the security of key actors in a number of crucial sectors and they provide for a similar logic by which EU countries identify and designate those key actors. At the same time, they present significant differences. Namely, the ECI Directive aims on enhancing the security of physical assets against threats such as terrorism and other intentional and unintentional man-made threats and natural disasters, while the NIS Directive focuses on the security of network and information systems against cyber-threats.

The ECI Directive is limited to the ECI, i.e.,, those infrastructures, the destruction/disruption of which would have a significant cross-border impact on at least two Member States, while the NIS Directive covers operators without explicitly requiring Member States to determine if negative cross-border effects can be anticipated in case of a disruption/destruction. Besides, the ECI Directive is focused on the protection of specific assets that provide certain essential services, while the NIS Directive takes a broader approach and consider essential services as a whole. When it comes to the sectoral scope of the two Directives, the ECI is limited to the energy and transport, while the NIS2 covers the sectors of energy, transport, banking, financial market infrastructure, health, drinking water supply and distribution and digital infrastructure.[221] Last but not least, the ECI Directive aims to establish physical protective arrangements, while the NIS Directive prescribes that operators must take risk management measures in relation to network and information systems with the aim to ensure the continuity of those services.

## 5.5 Information sharing

Information sharing is an important resource for CIs security and resilience, being key to understand the cyber incidents that have occurred as well as to identify possible mitigation measures. What is of primary importance is that information sharing regarding ECI occurs in an environment of trust and security.[222] That relationship of trust will allow companies and organisations to know that their sensitive and confidential data will be sufficiently protected.

Information sharing can occur in a lot of ways and can be internal, i.e., within the organisation or external, i.e., between or among several organisations, one or more CIs sectors and/or industries,

[221] Annex I, NIS2 Directive; Article 3(3), ECI Directive.
[222] Preamble para. 19, ECI Directive.

across a sector, between one or more organisations and law enforcement or regulators, etc. It can concern a range of important data, ranging from security practices, risks, threats and incidents occurred, to personal data, intellectual property as well as other confidential or business-related information. Information sharing is important for all types of incidents and threats. Whether there is a threat of something actually occurring or an incident that has actually occurred, both threats and incidents have indicators to help determine what may occur (in the case of a threat) or what has occurred (in the case of an incident).

In order to remain ahead of a threat, information must be shared in an accurate, timely and effective manner. For example, organizations can share information regarding incidents that they have experienced in order to warn others about them.[223]

Apart from the notification requirements described in the previous sections, the sharing of security-related information among CIs and with public authorities is not comprehensively regulated at the EU level. Nevertheless, cyberattacks are criminalised on a national, European and international level, and CIs progressively need to cooperate, either on a voluntary or mandatory basis, with national competent or law enforcement authorities for the prevention, detection, investigation and prosecution of cybercrimes constituted by cyber-attacks.[224] Such cooperation among ECIs as well as with European bodies and agencies including Europol,[225] its European Cybercrime Centre (EC3) and ENISA,[226] is encouraged and promoted.[227]

PRAETORIAN end-users, in their capacity as CI, may participate in the Critical Infrastructure Warning Information Network (CIWIN). The CIWIN network has been set up as a EC-owned protected public internet based information and communication system, and offers recognised members of the ECIs protection community the opportunity to exchange and discuss ECIs protection-related information, studies and/or good practices across all EU Member States.[228]

---

[223] Here it is good to note that the European Reference Network for Critical Infrastructure Protection[223] (ENRCIP) has the mission to foster the innovative, qualified, efficient, and competitive security solution, building a European network. Different Thematic Groups are existing, allowing the development of the best practices in different CIP area. See: https://erncip-project.jrc.ec.europa.eu/

[224] Daphné Van der Eycken, Ilaria Buri, Plixavra Vogiatzoglou, Anton Vedder, CyberSANE Deliverable D2.2 Legal and Ethical Requirements (2020), p.58.
[225] European Union Agency for Law Enforcement Cooperation.
[226] European Union Agency for Network and Information Security, https://www.enisa.europa.eu/.
[227] Daphné Van der Eycken, Ilaria Buri, Plixavra Vogiatzoglou, Anton Vedder, CyberSANE Deliverable D2.2 Legal and Ethical Requirements (2020), p.58.
[228] European Commission, Critical Infrastructure Warning Information Network (CIWIN). Available at: Critical Infrastructure Warning Information Network (CIWIN) (europa.eu)

# 6. Legal Framework on the Use of Drones

Since drones are planned to be used in the PRAETORIAN project as a part of the physical situation awareness system, this section gives an overview of the applicable international legal framework for unmanned aviation, including significant international treaties governing civil aviation as well as EU instruments and initiatives. National legislation will not be addressed, despite the fact that there may be important relevant types of legislation regarding drones across Member States. As a result, if drone technology is used, the consortium members are strongly advised to consult national legislation. Furthermore, this part will not examine the private international law components of liability and insurance, because the implementation of these laws is dependent on the specific context and, in many cases, national legislation.[229]

## 6.1 The International Legal Framework

For the time being there is no legal instrument regarding the safety of remotely piloted aircraft or including an official use of the term "unmanned aviation" on the international level. For this reason, the international instruments which may be considered applicable to drones will be briefly touched upon. The most prominent one is the Convention on International Civil Aviation (also known as the Chicago Convention) of 1944. [230] Under this convention, the operations of unmanned aircrafts in the territory of another state require the authorization of that state as Article 8 of the Chicago Convention stipulates,

> *"No aircraft capable of being flown without a pilot shall be flown without a pilot over the territory of a contracting State without special authorization by that State and in accordance with the terms of such authorization. Each contracting State undertakes to insure that the flight of such aircraft without a pilot in regions open to civil aircraft shall be so controlled as to obviate danger to civil aircraft."*

Since this convention governs international aviation, domestic operations will be exempted unless they fulfill the international standard (which is not frequently met for civil applications of remotely piloted aircraft, but it is easily met in military situations). In many circumstances, national law will

[229] Janja Cevriz, Plixavra Vogiatzoglou, Ivo Emanuilov, Laurens Naudts, Anton Vedder, SAURON Deliverable D3.2 Legal and Ethical Requirements (2017), p.60.
[230] ICAO, Convention on International Civil Aviation.

establish the appropriate regulations in terms of territorial scope and safety, and it will take into account the international aspect[231].

With regards to safety, there are no standards and recommended practices adopted at the international level but the Chicago Convention enshrines some general requirements for safety for every aircraft engaged in international navigation, and these requirements, to some extent, also apply to remotely piloted aircrafts.

In 2011, the International Civil Aviation Organization (ICAO) issued a circular titled 'Unmanned Aircraft Systems (RPAS)' to increase awareness about the integration of UAS into non-segregated airspace and at aerodromes.[232] The circular emphasizes the remote pilot's critical role in ensuring the safe and predictable operation of the aircraft as it interacts with other civil aircrafts and the air traffic management system, as well as the fact that the pilot of the remotely piloted aircraft should follow state instructions, including using electronic and visual means, and should be able to divert to a specified airport at the state's request.[233] The circular is a soft law that is meant to guide rather than obligate, but it underlines the difficulties of incorporating remotely piloted aircraft into the existing certification system.[234]

With regard to liability, although there are several international treaties addressing the issue of liability for damages in air law, their applicability in the context of remotely piloted aircrafts is heavily reliant on national legal constraints. As a category of liability, second-party liability refers to the carrier's or operator's liability for damages to passengers or goods, which applies when the parties have an existing contractual relationship. The 1999 Convention for the Unification of Certain Rules for International Carriage by Air (also known as the Montreal Convention), is the most recent international legal instrument that specifies some of the rules for second-party liability. It is not intended to unify the second-party liability regime in its entirety because it merely stipulates "certain rules."[235] On the other hand, third-party liability refers to the liability for compensation for persons who suffer damage

[231] Janja Cevriz, Plixavra Vogiatzoglou, Ivo Emanuilov, Laurens Naudts, Anton Vedder, SAURON Deliverable D3.2 Legal and Ethical Requirements (2017), p.61.
[232] ICAO Circular 328, Unmanned Aircraft Systems (UAS)
[233] ICAO Circular 328, Unmanned Aircraft Systems (UAS), p.11
[234] Janja Cevriz, Plixavra Vogiatzoglou, Ivo Emanuilov, Laurens Naudts, Anton Vedder, SAURON Deliverable D3.2 Legal and Ethical Requirements (2017), p.61
[235] Pablo Mendes de Leon, Benjamyn Ian Scott, "An Analysis of Unmanned Aircraft Systems under Air Law," in Drones and Unmanned Aerial Systems: Legal and Social Implications for Security and Surveillance, ed. Aleš Završnik (Cham: Springer International Publishing, 2016), p. 204.

caused on the surface and it is covered by the 1952 Convention on Damage Caused by Foreign Aircraft to Third Parties on the Surface (known as the Rome Convention). [236]

## 6.2 EU Legal Framework

The 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 (Basic Regulation), adopted on 4 July 2018, regulates the civil aviation in the EU and it has established the European Union Aviation Safety Agency (EASA). Although some general requirements have been set in the context of the unmanned aircraft in Section VII (Articles 55-58) and Annex IX, they are rather general, and many aspects are left to be regulated by the implementing and delegated acts. Two implementing regulations focusing on civil drones have particular importance at this point.

The basis for the safe operating of civil drones in European airspace is laid forth in EU Regulations 2019/947 and 2019/945[237]. They use a risk-based approach and do not differentiate between private and commercial civil drones' activity. They consider the civil drone's weight and specifications, as well as the operation it will perform. Regulation (EU) 2019/947, which has been in effect in all EU Member States as well as Norway and Liechtenstein since 31 December 2020 (soon to be expected to be applicable also in Switzerland and Iceland), covers the majority of civil drone operations and their risk levels. It distinguishes between three types of civil drone operations:

- The **"open" category** is for lower-risk civil drone activities in which safety is guaranteed as long as the civil drone operator follows the relevant requirements for the operation. There are three subcategories under this category: A1, A2, and A3. Because the operational risks in the "open" category are low, no operational authorization is necessary before taking off.
- The **"specific" category** covers more risky civil drone activities, where the drone operator ensures safety by acquiring an operational authorization from the national competent authority before beginning the operation. The drone operator must complete a risk assessment to receive the operating authorization, which will define the requirements for the safe operation of the civil drone(s).

[236] Janja Cevriz, Plixavra Vogiatzoglou, Ivo Emanuilov, Laurens Naudts, Anton Vedder, SAURON Deliverable D3.2 Legal and Ethical Requirements (2017), p.61

[237] Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft, OJ L 152, 11.6.2019, and Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems, OJ L 152, 11.6.2019. Available at: https://www.easa.europa.eu/document-library/easy-access-rules/easy-access-rules-unmanned-aircraft-systems-regulation-eu, last accessed: 10 May 2022.

- The safety risk is significantly higher in the **"certified" category**; hence, certification of the drone operator and its drone, as well as licensing of the remote pilot(s), is always necessary to assure safety.[238]

It is important to note that drone operators need to register in the country of their residence or of the principal place of business. Details regarding the registration process in each country can be seen on the websites of the National Aviation Authorities[239].

Furthermore, the Commission Implementing Regulation (EU) 2021/664 (U-space Regulation)[240], adopted on 22 April 2021, specifies and harmonizes the rules for manned and unmanned aircrafts to operate safely in the U-space airspace, with the objectives of preventing aircraft collisions and mitigating air and ground risks. To clarify, Article 2(1) of this regulation defines the U-space as "a UAS geographical zone designated by Member States, where UAS operations are only allowed to take place with the support of U-space services", and Article 2(2) defines a U-space service as "a service relying on digital services and automation of functions designed to support safe, secure and efficient access to U-space airspace for a large number of UAS". Thus, the regulatory framework for U-space aims to ensure safe aircraft (manned or unmanned) operations in all forms and in all areas, including the ones where heavier traffic is expected such as urban areas.[241]

Since the details of the use cases and of the drone operations are not specified yet, further specifications will not be provided here. However, it should be noted that Article 56(8) of the Basic Regulation stipulates that Member States can "*lay down national rules to make subject to certain conditions the operations of unmanned aircraft for reasons falling outside the scope of this Regulation, including public security or protection of privacy and personal data in accordance with the Union law*." Thus, the consortium partners should look for the related legal acts or provisions in national laws of Members States, which are not the subject matter of this deliverable, in addition to the EU regulations referred above.

[238] European Union Aviation Safety Agency (EASA), Civil Drones (Unmanned Aircraft). Last Access: 11 May 2022.
[239] See the list of the authorities of the EEA countries. Available at: https://www.easa.europa.eu/domains/civil-drones/naa, last accessed: 11 May 2022.
[240] Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space, OJ L 139, 23.4.2021. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0664. Last access: 11 May 2022.
[241] European Union Aviation Safety Agency (EASA), Civil Drones (Unmanned Aircraft). Last Access: 11 May 2022.

# 7. Ethical Framework

As the ethical framework has been analysed in D9.1 – Research Ethics and Privacy management, this section will focus on giving an overview of the results of D9.1. For a complete analysis, please refer to D9.1.

The PRAETORIAN consortium must carry out its research and actions in compliance with ethical principles, such as set out in the European Code of Conduct for Research Integrity guidelines.[242] The main areas that were identified to be relevant for the ethical analysis were: involvement of human participants, protection of personal data, societal impact, dual use and misuse.

Whenever **human beings are involved in the project**: information on privacy and confidentiality, and the evidence about the compliance with national and EU legislation should be provided to project participants. PRAETORIAN should develop a procedure for the identification and recruitment of research participants, while avoiding the participation of vulnerable individuals or groups and persons unable to give valid consent. If patient data collection and processing are necessary to fulfil the project objectives, this should be carefully assessed during the project and reported. Participants in the research should be involved in a voluntary way, free from any coercion or risk. For this reason, monetary compensation for participation should be avoided, but forms of in-kind compensation to participants for the time they have dedicated to the project can be considered. Potential research participants must be informed about the project, its purpose, methods and intended possible uses, but also about what their participation in the research entails and what risks are involved. This information must be provided to them in an accessible format.

Informed consent must be obtained. It is important to note that two types of informed consent exist, one is informed consent as ethical standard in research, the other informed consent as a legal basis for the processing of personal data.

**Protection of personal data**: data protection legislation should be taken into account for the PRAETORIAN technology and project research. The specifics can be found in section 3, but also in D9.1 and D11.3.

**Societal impacts**: Based on the Ethics Self-Assessment the research done in PRAETORIAN aims to address societal security needs and respect for private life and data protection. The aim is to innovate

[242] See European Commission 'Ethics', https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm and ALLEA, The European Code of Conduct for Research Integrity – revised edition, Berlin, 2017. Available at: https://www.allea.org/wp-content/uploads/2017/05/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017.pdf, last visited 18.5.2022.

functionalities and services to protect people and to offer complementary services that will enhance citizens' data protection and improve the physical and cyber-security of cities. This will be done by improving the coordination among public and private security operators to build a safe environment for citizens. The project dissemination activities will inform the citizens and will also be used to collect feedback.

**Dual use**: The risk of dual-use items is that they can be used for both civil applications and military purposes. D11.4 provides details on potential dual-use implications and risk-mitigation strategies of the project. It was stressed that special attention should be paid to potential Intangible Technology Transfers which can occur inadvertently by providing non-EU entities with technology. It was outlined that partners must be aware of the applicable frameworks to potential "exports" and their qualification as "exporters". Moreover, it was stipulated that in case a PRAETORIAN partner aims to export a dual-use item to a non-EU destination, they must first obtain the appropriate authorisation and collaborate with their competent national authority. They must also, at all times, exercise proper due diligence regarding potential dual-use risks and implications and they will have to continuously monitor and manage potential dual-use risks and implications throughout the PRAETORIAN project lifetime. In order to properly address the identified dual-use risks and implications, partners must implement appropriate measures (e.g., raising awareness, active measures, risk follow up). For these purposes, it was articulated that a PRAETORIAN dual-use risk monitoring and management strategy will be developed and kept up-to-date.

**Misuse**: A potential ethical risk would be the misuse of research findings. This has been addressed in D11.5. In order to identify and address risks of potential misuse of research findings in PRAETORIAN, a questionnaire, which was based on the EC guidelines on potential misuse of research, has been developed that has been circulated among all PRAETORIAN partners. Risks that were identified where the potential that the PRAETORIAN research can be considered to provide knowledge, materials, and technologies that could be channelled into crime or terrorism. Specifically, the research findings (e.g., , vulnerability and risk assessments), if they ended up in the wrong hands, could lead to physical or cyber-attacks on CIs by exploiting the identified weaknesses. It also involves technologies that can be used for surveillance purposes with the potential to curtail human rights and civil liberties. This applies to the video analytics software for physical intrusion detection and threat identification in particular, for which surveillance is the intended and lawful purpose. To address these risks, the PRAETORIAN consortium has implemented several measures, such as the appointment of a SAB, PSO and an Ethics Board to oversee the handling of sensitive information and address potential ethical issues. Multiple deliverables have also been made consortium confidential (limited dissemination) or classified as RESTREINT UE/EU RESTRICTED to protect and secure sensitive information that may be misused.

Partners involved in vulnerable research areas, i.e.,, IDEMIA, will also use synthetically generated 3D data to mitigate risks of potential misuse further. Finally, a PRAETORIAN misuse risk monitoring and management strategy will be developed and kept up to date.

# 8. Conclusion

PRAETORIAN aims to enable the security stakeholders of the CIs in Europe to manage the lifecycle of security threats, from the forecast, assessment and prevention to detection, response and mitigation, in a collaborative manner with the security teams from related CIs – being the CIs in the same or different sector. The strategic goal is to increase the security and resilience of ECIs, facilitating the coordinated protection of interrelated ECIs against combined physical and cyber threats. To this end, the project will provide a multidimensional (i.e.,, economic, technological, policy and societal) yet installation-specific toolset comprising: (i) a Physical Situation Awareness system, (ii) a Cyber Situation Awareness system; (iii) a Hybrid Situation Awareness system, which will include digital twins of the ECIs under protection; and (iv) a Coordinated Response system. The PRAETORIAN toolset will support the security managers of ECIs in their decision making to anticipate and withstand potential cyber, physical or combined security threats to their own ECI and other interrelated ECIs that could have a severe impact on their performance and/or the security of the population in their vicinity. The project will specifically tackle (i.e., prevent, detect, respond and, in case of a declared attack, mitigate) human-made cyber and physical attacks or natural disasters affecting ECIs. It will also address how an attack or an incident in a specific ECI can jeopardise the regular operation of other neighbouring/interrelated ECIs and how to make all of them more resilient by predicting cascading effects and proposing a unified response among ECI assisting First Responder teams.

This deliverable provides an analysis of the relevant legal and ethical frameworks applicable to PRAETORIAN throughout the project lifetime. More precisely, this document provides an overview of the international and European frameworks on privacy and data protection, cybersecurity, CIs) and use of drones. Particular attention has been given to the balancing of rights and interests, more specifically the rights of individuals (e.g., the right to privacy and data protection) and society (e.g., the protection of the EU critical infrastructures). It also provides the consortium members with an essential guidance on how to achieve the objectives of the PRAETORIAN research project in a legally and ethically compliant way.

It is noteworthy that this deliverable should be read in conjunction with the *Deliverable D9.1: Research Ethics and Privacy Management*. Furthermore, since the use cases of the PRAETORIAN project and their specifications have not been formed yet, detailed descriptions of the analysed legal requirements in the context of the project could not be provided in certain sections. These, as well as the legal requirements enshrined in national laws, should be further investigated by the consortium partners as soon as the use cases and their specifications are formed.

## Bibliography

**Legislation, Legislative Documents, Official Positions and Conventions**

Commission Implementing Regulation (EU) 2018/151- of January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact, OJ L 26/48, 31.01.2018.

Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft, OJ L 152, 11.6.2019. Available at: https://www.easa.europa.eu/document-library/easy-access-rules/easy-access-rules-unmanned-aircraft-systems-regulation-eu.

Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems, OJ L 152, 11.6.2019. Available at: https://www.easa.europa.eu/document-library/easy-access-rules/easy-access-rules-unmanned-aircraft-systems-regulation-eu.

Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space, OJ L 139, 23.4.2021. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0664.

Council of Europe, European Convention on Human Rights, 4 November 1950.

Council of Europe, The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), 28 January 1981.

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 OJ L 345/75 23.12.2008 (“ECI Directive).

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (“e-Privacy Directive”), OJ L 201, 31.07.2002.

Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the

execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/ 977/ JHA, OJ L 119, 4.5.2016 ("LED").

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 ("NIS Directive"), OJ L 194, 19.7.2016.

EC Staff Working Document on the free flow of data and emerging issues of the European data economy Accompanying the document Communication Building a European data economy, 10.1.2017 SWD(2017) 2 final, available at https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy.

European Commission, Communication, Building a European Data Economy, COM(2017) 9, 10.01.2017. Available at: https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy .

European Commission, Communication, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, COM(2019) 250, 29.05.2019. Available at: https://ec.europa.eu/digital-single-market/en/news/practical-guidance-businesses-how-process-mixed-datasets.

European Commission, Communication: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, 2016.

European Commission, Commission Staff Working Document, Evaluation of Council Directive 2008/114 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve protection, 23.07.2019. Available at: 20190723_swd-2019-308-commission-staff-working-document_en.pdf (europa.eu).

European Commission, Commission staff working document Impact assessment, accompanying the document for the proposal for a Directive of the European parliament and of the Council on the resilience of critical entities, 16.12.2020. Available at: impact_assessment_swd-2020-358.pdf (europa.eu).

European Commission, EU cybersecurity initiatives, working towards a more secure online environment, 2017.

European Commission, The EU's Cybersecurity Strategy for the Digital Decade, Shaping Europe's digital future, 2020.

European Commission, High Representative of the EU for Foreign Affairs and Security policy, Joint Communication, Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace, Brussels, 7.2.2013, JOIN (2013).

European Union Aviation Safety Agency (EASA), Civil Drones (Unmanned Aircraft)

EU, Charter of the Fundamental Rights of the European Union, OJ C 326, 26 October 2012.

ICAO Circular 328, Unmanned Aircraft Systems (UAS), 2011.

ICAO, Convention on International Civil Aviation, Doc 7300/9, 9th edition, 2006.

International Maritime Organization, International Convention for the Safety of Life at Sea (SOLAS), 1 November 1974.

Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, 16.12.2020.

Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities, COM(2020) 829 final, (CER Directive), 16.12.2020.

Proposal for a Regulation 2017/0003 concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (e-Privacy Regulation).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016.

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018.

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), OJ L 151/15, 7.6.2019.

UN, Universal Declaration of Human Rights, 10 December 1948.

**Regulatory Guidance**

Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679, 4 October 2017.

Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, 536/14/EN, WP 21, Brussels, 27 Feb 2014.

Cooperation Group, Reference document on security measures for Operators of Essential Services, 01/2018.

Cooperation Group, Reference Document on Incident Notification for Operators of Essential Services, 02/2018.

European Data Protection Board, Guidelines 10/2020 on restrictions under Article 23 GDPR, Version 2.0, adopted on 13 October 2021.

ENISA, Crossing a bridge: the first EU cybersecurity certification scheme is availed to the Commission, 2021. Available at: https://www.enisa.europa.eu/news/enisa-news/crossing-a-bridge-the-first-eu-cybersecurity-certification-scheme-is-availed-to-the-commission.

ENISA, Cybersecurity Certification: Candidate EUCC Scheme, 2020. Available at: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme.

ENISA, Report on Public consultation on the draft candidate EU Scheme, 2021. Available at: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1/.

ENISA, Cybersecurity Certification, EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS, V.1.1.1, May 2021. Available at: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1.

European Commission, The EU cybersecurity certification framework, Shaping Europe's framework, 2022. Available at: The EU cybersecurity certification framework | Shaping Europe's digital future (europa.eu).

European Data Protection Board, Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR, 2.9.2020.

European Data Protection Supervisor, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11.4.2017. Available at: https://edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf

Report on Public consultation on the draft candidate EU Scheme, 2021.

**Cases**

CJEU:

C-131/12 Google Spain and Google [2014] EU:C:2014:317.

C-203/15 and C-698/15 Tele2 Sverige AB v Postoch telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, [21 December 2016] ECLI:EU:C:2016:970 ("Tele2").

C-210/16, Wirtschaftsakademie Schleswig-Holstein [2018] ECLI:EU:C:2018:388.

C-293/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [8 April 2014] ECLI:EU:C:2014:238 ("Digital Rights Ireland").

C-362/14 Maximillian Schrems v Data Protection Commissioner [06 October 2015] ECLI:EU:C:2015:650 ("Schrems").

Opinion 1/15 26 July 2017, ECLI:EU:C:2017:592 ("Opinion 1/15").

ECtHR:

Case of Roman Zakharov v. Russia, App. No 47143/06 [04 December 2015] ECLI:CE:ECHR:2015:1204JUD004714306 ("Zakharov").

Case of Szabó and Vissy v. Hungary, App. No 37138/14, Final Text 06 June 2016, ECLI:CE:ECHR:2016:0112JUD003713814 ("Szabó").

**Secondary Sources**

Alessandro Bruni, Promoting Coherence in the EU Cybersecurity Strategy, in Anton Vedder, Jessica Schroers, Charlotte Ducuing and Peggy Valcke (eds.), Security and Law, Legal and Ethical Aspects of public Security, Cyber Security and Critical Infrastructure Security, Intersentia, 2019.

Daphné Van der Eycken, Ilaria Buri, Plixavra Vogiatzoglou, Anton Vedder, CyberSANE Deliverable D2.2 Legal and Ethical Requirements,2020.

Dimitra Markopoulou, Vagelis Papakonstantinou, Paul de Hert, The EU Cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, Computer Law and Security Law Review 35,2019.

EU Agency for Fundamental Rights, Handbook on European Data Protection Law, Luxembourg, Publications Office of the European Union, 2018.

Finck, Michèle, and Frank Pallas, They Who Must Not Be Identified - Distinguishing Personal from Non-Personal Data Under the GDPR, SSRN Electronic Journal, 2019.

Janja Cevriz, Plixavra Vogiatzoglou, Ivo Emanuilov, Laurens Naudts, Anton Vedder, SAURON Deliverable D3.2 Legal and Ethical Requirements,2017.

O. Mironenko Enerstvedt, Aviation Security, Privacy, Data Protection and other Human Rights: Technologies and Legal Principles, SPRINGER, Law, Governance and Technology Series, Sub-series: Issues in Privacy and Data Protection 37, 2017.

Pablo Mendes de Leon, Benjamyn Ian Scott, "An Analysis of Unmanned Aircraft Systems under Air Law," in Drones and Unmanned Aerial Systems: Legal and Social Implications for Security and Surveillance, ed. Aleš Završnik,Cham: Springer International Publishing, 2016.

Plixavra Vogiatzoglou, Anton Vedder, SAURON Deliverable D3.5 Legal Requirements Specifications, 2018.

Rocher, Luc, Julien M. Hendrickx, and Yves-Alexandre de Montjoye, Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models, Nature Communications 10, no. 1, December 2019, 3069.

**Websites**

European Union Agency for Law Enforcement Cooperation, https://www.europol.europa.eu/.

European Union Agency for Network and Information Security, https://www.enisa.europa.eu/.