Cyber Security for Europe

D4.2

Legal Framework

Document Identification	
Due date	31st January 2020
Submission date	31st January 2020
Revision	1.1 (15th September 2020)

Related WP		Dissemination Level	CO
Lead Participant	POLITO	Lead Author	Dr. Alessandro Mantelero
Contributing Beneficiaries	POLITO, FORTH, UM	Related Deliverables	

Abstract:

This report deals with legal issues related to data security and cybersecurity from a business perspective, mapping the relevant legal and regulatory framework for the roadmapping process and linking it to the most important technological and organizational solutions supporting its implementation. The report summarises the main findings of Task 4.2 (M1-M12).

Through a functional analysis of the legal framework, the deliverable reveals the existing interconnections between the different legal instruments and the technology-focused backbone of the EU approach in this field. This crosscutting analysis, based on an interdisciplinary study, has made it possible to identify the key elements of the different legal provisions that are crucial for a data security and cybersecurity strategy.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

The flourishing of a mature and strong cybersecurity strategy for the data economy necessarily requires an appropriate regulatory framework. A framework as such cannot be limited to general cybersecurity conventions or regulations focused on certain cybersecurity issues (e.g. Regulation (EU) 2019/881 of 17 April 2019), but should have a broader perspective aiming to create a legal ecosystem focused on security and data protection.

From this standpoint, the following pages will present a legal and IT analysis of the unique regulatory environment which the EU legislator provides to companies that aim to play an active role in the digital economy. The deliverable will therefore focus on the General Data Protection Regulation (GDPR), the Network and Information Security Directive (NIS), the Payment Services Directive (PSD2), the Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation), and the proposed ePrivacy Regulation.

Adopting a *methodological approach* based on interdisciplinary research in the field of law & technology and on a crosscutting analysis of the different legal instruments, this study reveals the existing interconnections between these directives and regulations, identifying the common core of these different regulatory instruments. A common core that highlights the unique nature of the EU framework, which promotes fundamental rights through technology, fostering the development of cybersecurity research based on a by-design approach and safeguarding individual rights and societal interests in the digital economy.

The *results* of this crosscutting and comparative study show that all the legal provisions exanimated in this analysis, explicitly or implicitly, require the development of specific technologies for cybersecurity and data security. In addition, the framework provided by these different legal sources is not a patchwork, but a coordinated harmonious model, in which similar measures and procedures are required by different regulations to address issues related to the common core of these regulations.

This common core is based on five main pillars: risk-based approach, by-design approach, reporting obligations, resilience, and certification schemes. From a technology standpoint, the solutions that are necessary to meet the legal requirements related to these pillars confirm the existing crossover between these directives and regulations, as many of these legal requirements are achieved by the same technologies.

This uniformity demonstrates the existence of a fil rouge that characterises the whole approach adopted by the EU legislator in the broad field of data processing and cybersecurity within the context of the digital economy. This undoubtedly contributes to establishing a clear and unique framework for the development of a roadmap for the implementation of the Network of Competence Centres.

Document information

Contributors*

Name	Partner
Dr. Alessandro Mantelero	POLITO
Nicole Monte	POLITO
Meltini Christodoulaki	FORTH
Dr. Marko Hölbl	UM

Reviewers

Name	Partner
Pasquale Annicchino	Archimede
Jos Dumortier	Timelex

History

0.1	17.12.2019	Alessandro Mantelero	1st Draft
0.2	18.12.2019	Alessandro Mantelero	2nd Draft with suggestions from WPL and PC
0.3	15.01.2020	Alessandro Mantelero	3rd Draft incorporating the review feedback provided by Pasquale Annicchino
1.0	28.01.2020	Alessandro Mantelero	4th Draft incorporating the review feedback provided by Prof. Dr. Jos Dumortier
1.1	15.09.2020	Alessandro Mantelero Ahad Niknia	Minor corrections regarding the review comments

* The authors are grateful to Avv. Giuseppe Vaciago for the comments and suggestions provided about sections 3, 4 and 5 of this deliverable, and to Dr. Maria Samantha Esposito (Politecnico di Torino) for her contribution to section 2.

List of Contents

List of Figures

List of Tables

Glossary of Terms*

Advanced electronic seal
An electronic seal, which meets the requirements set out in Article 36 of eIDAS Regulation.

Advanced electronic signature
An electronic signature which meets the requirements set out in Article 26 of eIDAS Regulation.

Authentication
An electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed.

Biometric data
Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Certificate for electronic seal
An electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person.

Certificate for electronic signature
An electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person.

Consent
Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

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

Creator of a seal
A legal person who creates an electronic seal.

Cross-border processing
Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State.

* This glossary is based on the definitions provided by EU secondary legislation, namely the GDPR, the NIS directive, the PSD2 directive, and the eIDAS regulation.

Processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Data concerning health

Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Data Processing

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

Electronic identification

The process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person.

Electronic identification scheme

A system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons.

Electronic seal

Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.

Electronic seal creation data

Unique data, which is used by the creator of the electronic seal to create an electronic seal.

Electronic signature

Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.

Electronic signature creation data

Unique data which is used by the signatory to create an electronic signature.

Electronic signature creation device

Configured software or hardware used to create an electronic signature.

National strategy on the security of network and information systems

A framework providing strategic objectives and priorities on the security of network and information systems at national level.

Network and information system

a. An electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC; or
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; or
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.

Operator of essential services

A public or private entity of a type referred to in Annex II of NIS Directive, which meets the criteria laid down in Article 5(2) of NIS Directive.

Person identification data

A set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established.

Personal data breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Personal data

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processor

A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Profiling

Any form of automated processing of personal data consisting of the use 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.

Pseudonymisation

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

Qualified certificate for electronic seal

A certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III of eIDAS Regulation.

Qualified certificate for electronic signature

A certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I of eIDAS Regulation.

Qualified electronic seal

An advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal.

Qualified electronic signature creation device

An electronic signature creation device that meets the requirements laid down in Annex II of eIDS Regulation.

Qualified electronic signature

An advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.

Qualified trust service provider

A trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body.

Qualified trust service

A trust service that meets the applicable requirements laid down in this Regulation.

Security of network and information systems

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.

Supervisory authority

An independent public authority which is established by a Member State pursuant to Article 51 GDPR.

Trust service

An electronic service normally provided for remuneration which consists of:

a. the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
b. the creation, verification and validation of certificates for website authentication; or
c. the preservation of electronic signatures, seals or certificates related to those services.

Trust service provider

A natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider.

1 Introduction

This report summarises the main findings of Task 4.2 (M1-M12), which focuses on legal issues, and maps the relevant legal and regulatory framework for the roadmapping process.

Two are the main goals of this task: (i) to define the existing legal framework within which the roadmapping work will proceed, and (ii) to identify the elements (e.g. fostering the development of privacy enhancing technologies) that the unique European legal and regulatory requirements (i.e. GDPR, NIS directive, PSD2 directive, eIDAS regulation and the proposed ePrivacy Regulation) offers as a significant advantage in developing the Roadmapping.

Both these goals have been achieved through a functional analysis of the legal framework, adopting a business perspective. This perspective, which does not include the Cybersecurity Act or other regulatory instruments on law enforcement and intelligence services, aims to provide concrete guidance to both companies and research centres to develop policies oriented towards cyber security and data security. This will help the different actors in the digital economy to deeply root these policies in their practices, products and services, in line with the suggested by-design approach.

The analysis conducted in Task 4.2 does not follow the traditional approaches of legal commentaries but focuses on the relationship between the formal requirements of EU legislation and the related technical means necessary to implement them. This different methodological approach, based on an interdisciplinary study, has made it possible to identify the key elements of the different legal provisions that are crucial for a data security and cybersecurity strategy.

This crosscutting analysis has also revealed the existing interconnections between the different legal instruments and the technology-focused backbone of the EU approach in this area. This highlights the unique nature of the EU framework which fosters fundamental rights through technology and, as a result, boosts the development of data security and cybersecurity research based on a by-design approach, which safeguards individual rights and societal interests in the digital economy.

From this perspective, the research conducted by the Polytechnic University of Turin (POLITO) has been centred on the GDPR (General Data Protection Regulation), PSD2 Directive, eIDAS Regulation and NIS Directive, which represent the key elements of digital ecosystem regulation. In addition, this deliverable includes a focus on the future evolution of this regulatory framework in the field of online communications (ePrivacy regulation), based on the research carried out at FORTH.

Finally, the research team of the University of Maribor has analysed the most important technologies to comply with the EU regulations discussed in the previous sections, giving an indication of which legal requirements each technology or solution can help achieve. This section is also a good list of important research fields to support the implementation of the regulations in organizations and can serve as an outline for the research roadmap in cybersecurity and privacy.

The research conducted in Task 4.2 demonstrates that the existing legal requirements and, more in general, the EU framework provide a significantly favourable environment for the development of the roadmapping process and, from a technological perspective, contributes to shaping this process along specific main axes, in terms of cybersecurity research and development.

More specifically, the comparative analysis of the different legal sources has identified three main elements of the EU regulatory approach: an adequate balance between principles-based provisions and technical rules; a variety of technological solutions considered by law as crucial to achieve the EU objectives in the field of data protection and data security; and a clustering of the entire legal framework around five core elements (risk assessment, by-design approach, reporting obligations, resilience, and certification schemes).

This report moves from the general framework provided by the GDPR (Section 2), which sets out key principles concerning data processing, to sector-specific regulations (PSD2 Directive, eIDAS Regulation and NIS Directive) where these principles are applied in detail (Sections 3-5). The report also briefly considers the proposed ePrivacy Regulation (Section 6). In dealing with each legal instrument, after a brief introduction, the analysis focuses on the relevant provisions concerning cybersecurity obligations and provides an outline of them in a table showing the relationship between legal provisions and their technological and organisational implementations.

Following this legal analysis, Section 7 considers the most important technical solutions to support the regulations discussed in the previous sections. This is an extensive – though not exhaustive – list, designed to present the most important technologies and measures needed to meet the legal requirements as set by the GDPR, NIS Directive, PSD2 and eIDAS. Finally, in Section 8, we compare the results of the analysis of the different regulatory and technological instruments conducted in the previous sections, drawing some conclusions on the common core of the EU approach, which can also contribute to the future regulatory strategies of policy makers.

2 The General Data Protection Regulation Framework

2.1 Data protection regulations and Regulation (EU) 2016/679: an overview.

The need to ensure the protection of personal data first arose in the 1950s when the information process started. The migration from dusty paper archives to computer memories was a significant change, permitting the aggregation of a great deal of data about citizens. In that period, information was in the hands of a just few bodies, in particular of governments and big corporations, which were able to support the investments required by the new technological scenario. For this reason, the first national regulations represented the answer to the rising concern of citizens about social control. It was no longer only a question of protecting the right to privacy, but also of providing citizens with adequate protection in relation to the processing of their personal data[1].

In this context, the main purpose of regulations was to increase the level of transparency about data processing, giving citizens the opportunity to know who was able to monitor them, which kind of data were collected and for which purposes (the main protections offered by the first generations of data protection regulations concerned, in particular, transparency, access and control). Over time, the technological framework was characterized by several changes which forced legislators to intervene with different rules in response to the different needs arising from the use of citizens' personal information.

The first EU legal instrument on data protection was Directive 95/46/EC[2], which came into effect at a time when several Member States had already adopted national data protection laws. This Directive emerged from the need to harmonise these laws to ensure a high level of protection and the free flow of personal data among the different Member States[3]. It established a detailed and comprehensive data protection system in the EU. However, even though it was meant to provide complete harmonisation between national laws, it did not prevent fragmentation among Member States' legislation on data protection. In accordance with the EU legal system, the Directive was not directly applicable, but it had to be transposed into the national laws of the Member States. Inevitably, this caused different implementations of the general framework on data protection and resulted in both legal uncertainty and burdensome procedures for businesses operating across Europe. Legal uncertainty also affected data subjects, undermining their trust in data processing and online activities, regarding the security and protection of their data and rights. As a result, all these factors contributed to hindering the development of the data economy.

[1] The right to privacy and the right to personal data protection, although closely related, are distinct rights, concerning different aspects (they are explicitly protected as distinct fundamental rights, for example, in the Charter of Fundamental Rights of the European Union: see Article 7 and Article 8). The right to privacy, also referred to as the right to respect for private life, consists of a general prohibition on interference, subject to some public interest criteria that can justify interference in certain cases. On the contrary, the protection of personal data protects individuals whenever their personal data are processed, regulating the use of this information.

[2] Directive 95/46/CE of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[3] For more references see European Union Agency for fundamental rights (FRA), *Handbook on European data protection law*, 2018, available at https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law, last access 5 September 2019.

European data protection law is now enshrined in Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter also GDPR). The Regulation came into force on 25 May 2018, replacing the former Directive 95/46/EC, in order to address the new challenges posed by the rapid development of new technologies and increasing globalisation.

In this perspective, one of the two main goals of the GDPR is to deal with the new risks posed by technological evolution to the rights and freedoms of individuals. The GDPR stresses the need to protect individuals[4]' personal data[5] from the risks posed by data processing[6], considering the right to protection of personal data as a fundamental right like the Charter of Fundamental Rights of the European Union[7]. However, the GDPR does not only take into account the right to the protection of personal data, indeed the Regulation explicitly states that it is not an absolute right, but that it must be balanced against other fundamental rights and freedoms, such as the respect for private and family life, home and communication, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial and cultural, religious and linguistic diversity (Recital 4).

The second main goal of the GDPR consists in facilitating the flow of data across the Union, in order to ensure the development of European data economy and the creation of a digital single market. In this respect, Directive 95/46/EC needed to be superseded because, as already mentioned, it was the cause of fragmentation in the implementation of data protection across the Union. On the contrary, the GDPR aims to offer an effective common framework for the protection of the fundamental rights and freedoms of European citizens with regard to the processing of their personal data. Unlike directives, regulations are directly applicable under EU law; there is no need for national implementation. In this way, the GDPR establishes a single set of data protection rules across the EU, promoting an environment of legal certainty from which economic operators and **data subjects**[8] may benefit[9].

The Regulation reaffirms the traditional principles relating to personal data processing:

[4] The GDPR takes into account data processing relating only to **natural persons** and it applies only to living beings.
[5] According to the Regulation "**personal data**" is any information relating to an identified or identifiable natural person, see Article 4 no. 1. The European data protection law does not apply, therefore, to **anonymous data.** The process of anonymising data means that all identifying elements are eliminated from a set of personal data so that the data subjects is no longer identifiable (Recital 26 of the GDPR; see also Article 29 Data Protection Working Party, *Opinion 5/2014 on Anonymisation Techniques*, WP216, 10 April 2014).
[6] Under the GDPR "**data processing**" concerns any operation performed on personal data, whether or not by automated means (e.g. collection, recording, storage, consultation, disclosure by transmission, etc.), see Article 4 no. 2.
[7] See Article 8 ECHR.
[8] The term "data subject" identifies the person to whom the data processed refer.
[9] However, the Regulation leaves Member States a margin of discretion for specific provisions in some sectors (see, in particular, Recital 10 of the GDPR).

- **lawfulness, fairness and transparency principle:** personal data must be processed lawfully[10], fairly and in a transparent[11] manner in relation to the data subject.
- **purpose limitation principle**: personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes:
- **data minimisation principle:** personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- **accuracy principle:** personal data must be accurate and, where necessary, kept up to date;
- **storage limitation principle:** personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Moreover, of particular importance in the GDPR is the **principle of accountability**, according to which the controller[12] shall be responsible for, and be able to demonstrate compliance with data protection regulation. This is not a new principle in the data protection framework, but the GDPR reinforces the relevant provisions.

In the GDPR, as in the Directive, security of data processing plays a central role in the regulation: security – in terms of data **integrity and confidentiality –** is one of the core requirements concerning data processing[13].

In this context, security obligations aim not only to prevent data breaches and cyber-attacks but also to achieve the broader goal of ensuring the functioning of ICT systems, their interoperability and, more in general, their reliability. Therefore, ensuring data security is not an isolated obligation grounded only on a few specific provisions in the GDPR, but should be considered in the broader perspective of the accountability framework which data controllers should put into practice, according to the GDPR.

Controllers[14] are required to put into place both **organisational and technical measures** in order to ensure an appropriate level of security of personal data and, therefore, the protection of a data subject's fundamental rights and freedoms. In this context, it should be noted that the GDPR stresses the need to consider privacy and data protection at the design phase and throughout the entire data lifecycle, as well as the need to put into place appropriate technical and organisational security measures to implement privacy and data protection principles.

[10] Lawful processing requires the consent of the data subject or another legitimate ground provided in the data protection legislation (i.e. when processing is necessary for compliance with a legal obligation or for the purpose of the legitimate interests of the Controller or third parties).
[11] Controllers must take any appropriate measure in order to keep the data subjects informed about how their data are being used.
[12] "Controller" is the natural or legal person, which, alone or jointly with others, determines the purposes and means of the processing of personal data (Article 4 no. 7).
[13] Article 6 (1)(f).
[14] It should be noted that the Regulation also extends data security responsibility to data processors. A "processor" is defined under the GDPR as someone who processes personal data on behalf of a Controller (Article 4, no. 8).

This particular attention to technology development in order to address privacy and data concerns is not new. Since the end of the 1970s, computer scientists and legal scholars developed researches to address privacy concerns through technological solutions, which aimed to reduce the amount of processed data (data minimisation), make anonymous communications possible and, more in general, create a wide range of privacy-friendly technologies in different sectors. This approach was based on a paradigm change, in which technology development was not only the potential cause of the increasing privacy concern but it could also be part of the solution. These different solutions and scientific contributions gave rise to the so-called Privacy Enhancing Technologies (PETs), a set of different technological solutions oriented to minimise the privacy risk to individuals[15].

Building on the PETs experience, more recently, the "privacy by design" approach was elaborated as a broader and proactive approach that seeks to embed privacy as a value and binding requirement in products and services from the very beginning of their development.[16] According to this line of action, privacy should be embedded into design specifications of information technologies, infrastructures and practices, and should underpin their entire lifecycle.

Some elements of the principle of privacy by design could already be found in the Data Protection Directive 95/46/EC (see Recital 46 of the Directive). However, the GDPR (Article 25) addresses for the first time data protection by design as a legal obligation for data controllers and processors, making an explicit reference to data minimization and the possible use of pseudonymisation. Moreover, the GDPR also introduces the obligation of data protection by default, going a step further stipulating the protection of personal data as a default property of systems and services. As a result, controllers are required to put into place various technical and organisational measures to effectively integrate the data protection safeguards into processing activities in order to comply with the Regulation and protect the fundamental rights of the individuals whose data are processed.

In this context, the GDPR places special emphasis on the notion of risk. In particular, the GDPR goes beyond the traditional idea of risk in terms of data quality and data security and takes into account the broader impact of data processing on human rights and fundamental freedoms.

In this perspective, the Regulation assigns a significant role to risk analysis and risk management, introducing more detailed provisions which better specify the general requirements that were present in the repealed Directive 95/46/EC[17]. In this regard, the GDPR adopts a **risk based-approach** not only in defining specific data security obligations but requiring a risk management strategy, as demonstrated by the controller's obligations under the provisions concerning the records of the processing activities (Article 30),

[15] See, European Data Protection Supervisor (EDPS), *Opinion 5/2018. Preliminary Opinion on privacy by design*, 31 May 2018, available at https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf, last access 1 September 2019, 3.

[16] The term "privacy by design" was originally used by the Information and Privacy Commissioner of Ontario Ann Cavoukian (in 1997), who emphasized the need to be proactive in considering the privacy requirements as of the design phase throughout the entire data lifecycle. See, amongst other, Ann Cavoukian, 'Privacy by design: the definitive workshop. A foreword' (2010), IDIS, 3, 2, 247-251.

[17] See Mantelero A., 'Comment to Article 35 and 36, in Cole, M., Boehm, F. (eds.). GDPR Commentary, Edward Elgar Publishing, 2019, Forthcoming.

data protection impact assessment, prior consultation (Articles 35 and 36), and data breaches (Articles 33 and 34). This strict relationship between security and risk management is also evident in the soft-law and co-regulatory instruments of the GDPR, such as the use of certification and codes of conduct (Articles 40 and 42). Although the Regulation does not provide specific standards or risk management methods, it contains relevant procedural rules. In particular, in establishing the procedure to be followed when carrying out an impact assessment, the GDPR prescribes a multi-stage process, in accordance with traditional risk analysis models. This process includes an analysis of the envisaged processing, an assessment of the risks to the individual's rights and freedoms, the identification of the measures to address the risks to the individual's rights and freedoms, the verification of the effectiveness and periodic updating of measures[18].

2.2 GDPR and security obligations

The Regulation highlights several aspects of data processing and of the processing environment that require adequate security measures and continuous monitoring. In this perspective, this section identifies the various security requirements of the GDPR, considering the issues concerning data governance and task management, technical and organisational security measures, and risk management measures.

2.2.1 Data governance obligations and a company's organizational structure

Access control and security. In order to ensure the integrity and confidentiality of personal data, the GDPR requires controllers and processors to, amongst other things, adopt appropriate security measures for **protection against unauthorised access to systems** [see **Recital 39; Article 5 (1)(f)**].

a. Data minimisation and data storage limitation. With the aim of reducing the consequences of system incidents or personal data breaches, the GDPR requires controllers to limit the amount of data to process unless it is strictly necessary: only personal data that are necessary for each specific purpose of the processing may be processed ('data minimisation' principle) [**Article 5 (1)(c)]**. Moreover, personal data should not be retained for longer than necessary in relation to the purposes for which they were collected, or for which they will be further processed ('storage limitation' principle[19]) [**Article 5 (1)(e)**].

[18] See 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*", Adopted on 4 April 2017, as last revised and adopted on 4 October 2017, WP 248 rev.01, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236, last access 2 September 2019.

[19] ENISA, *Guidelines for SMEs on the security of personal data processing*, December 2016, https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing, last access 5 September 2019, 45.

b. Definition of roles and responsibilities. From an organisational perspective, an important security measure is the **definition of roles and responsibilities** of the entities involved in data processing [**Recital 79**].

GDPR requires data controllers to carefully select data **processors:** processors have to provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subject **[Article 28].**

Both controllers and data processors must put into place specific measures to ensure that the **personnel** involved in data processing are properly informed on specific data protection legal obligations and, in particular, about their duty to confidentiality **[Article 32 (1)(4)]**.

DPO
Data Protection Officer (DPO) (**Articles 37-39**) plays a central role in the processing model outlined in the GDPR. The DPO has to monitor compliance with the Regulation in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations and the related audits. The designation of a Data Protection Officer is mandatory for certain types of data processing operations (e.g. large scale monitoring activities, processing of special categories of data, etc.). Data controllers and processors have to appoint a DPO on, amongst other things, the basis of their professional qualities and expert knowledge of data protection law and practices.

c. Data processing monitoring [Article 30]. This is another important duty concerning an organization's security framework**.** According to this provision, controllers and, where applicable, processors, shall maintain a **record of processing activities** which shall include, amongst other things, the registration of the technical and organisational security measures adopted to protect the personal data. This is an important security provision which consents to regularly monitor the security measures in place.

d. Codes of conduct and Certification. Adherence to an approved **code of conduct** [**Article 40**] or an approved **certification mechanism**[20] [**Article 42**] may be used by controllers as an element by which to demonstrate compliance with the Regulation of processing operations and their conformity to the security requirements set out in this legislation [see also Recital 77 and Articles 24 (3), 25 (3) and 32 (3)][21].

[20] I.e. ISO 27001.

[21] For example, a code of conduct may specify the application of the Regulation, with regard to, for example: the pseudonymisation of personal data; the exercise of the rights of data subjects or the measures to ensure security of processing referred to in Article 32, see Article 40 (2).

2.2.2 Security measures

Article 32 contains the main security obligations in relation to the measures to be taken to ensure data protection. The GDPR requires data controllers and, where applicable, data processors, to ensure that **appropriate technical and organisational measures** are in place to protect personal data.

The Regulation does not stipulate a specific set of security measures but rather expects data controllers and data processors to take 'appropriate' actions. These measures shall take into account: the state of art, the costs of implementation; the nature, scope, context, and purposes of the processing; the risk of varying likelihood and severity for the rights and freedoms of natural persons [Article 32 (1)].

In assessing the appropriate level of security, controllers must take into account, among other things, the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed [Article 32 (2)].

The GDPR provides some recommendations as to what type of security measures may be considered 'appropriate' [Article 32 (1) (a-d)].

In this context, the GDPR firstly refers to pseudonymisation and encryption as examples of appropriate security measures[22] [Article 32 (1)(a); Recitals 28, 83].

Moreover, according to the GDPR security measures have to ensure: "*the ongoing confidentiality, integrity, availability and resilience of processing systems and services*" [Article 32 (1)(b)] and "*the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*" [Article 32 (1)(c)].

Finally, a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures must also be adopted to ensure the security of the processing [Article 32 (1)(d)].

2.2.3 Risk management measures

a. Data protection by design and by default. Article 25, explicitly adopting the privacy by design approach, requires data controllers to put into place, both at the time of the determination of the means of the processing and at the time of the processing itself, technical and organisational measures to implement data protection in an effective manner and to integrate the necessary safeguards into the processing (principles of data protection by design and by default[23]). This obligation therefore covers the amount of personal data collected, the extent of the processing, the period of storage and its accessibility. As a result, controllers are required to adopt various technical and organisational measures to ensure compliance with GDPR provisions. These measures shall be identified taking into account the state of art, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks for the

[22] See Long, RM., Blythe, F., Raul, A. C. 2018. European union overview. In Raul, A.C. (ed), *Privacy, Data Protection and Cybersecurity law Review*. The Law Reviews, 5th edition.
[23] See above Section 2.1.

rights and freedoms of individuals. Moreover, the Article states that, by default, only the personal data that are necessary for each specific purpose of the processing may be processed.

The Regulation does not suggest a list of specific mechanisms to integrate data protection in the development of new processes, technologies or other solutions. However, it gives relevant indications that highlight the need to define specific security requirements from the early stages of data processing. In particular, this provision indicates **pseudonymisation** and **data minimisation** as measures capable of effectively implementing data protection.

PETs
Although the GDPR does not provide a direct reference to Privacy Enhancing Technologies (PETs), its specific provisions for data protection by design and by default (Article 25) put clear emphasis on the engineering of privacy requirements into IT systems and services. As already mentioned, PETs are those technologies that help to embody data protection principles by minimising personal data use, maximising data security and empowering individuals[24]. In this sense, PETs can be considered as quality basic building blocks for engineering privacy and, in particular, for data security. There exist several examples of PETs that can help to address the various GDPR requirements and, in particular, obligations relating to the security of personal data. PETs may consist of systems that can be used before any personal data is used (e.g. technologies that can help controllers to respect data minimisation, anonymisation or limitation of use principles or the e-consent mechanism) or systems that help controllers to safeguard privacy while personal data is being processed (e.g. technologies that help to ensure data quality and verification; technologies that help to put into place restrictions on access to personal information or technologies that ensure protection of personal data against unlawful processing, such as encryption tools or tools to prevent hacking when information is transmitted over the Internet, etc.).[25] However, it is important to stress that PETs are not limited to pieces of software or hardware, but include procedures and management systems as well.

[24] See, Information Commissioner's Office – ICO, *Data protection by design and default*, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/, last access 2 September 2019.

[25] Some examples can be found in: Cranium Campus, *Summary of Privacy Enhancing Technologies – A Survey of Tools and Techniques*, available at https://craniumcampus.eu/summary-of-privacy-enhancing-technologies-a-survey-of-tools-and-techniques/, last access20 September 2019; see also London Economics. 2010. *Study on the economic benefits of privacy-enhancing technologies (PETs)*, available at https://londoneconomics.co.uk/wp-content/uploads/2011/09/17-Study-on-the-economic-benefits-of-privacy-enhancing-technologies-PETs.pdf, 15, where are cited, for example, technologies able to protect the content of Internet conversations (e.g. Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

Moreover, it should also be noted that PETs can help organisations not only to ensure the protection of personal data but also to ensure compliance with the GDPR in relation to various other aspects[26]. This is the case, for instance, of the:

- Controller's obligation to ensure informed consent [Recitals 32, 33, 42, 43; Article 7]: PETs can help to ensure that the data subject's consent to data processing is an informed one.
- Controller's transparency obligations in relation to the data subjects [Recital 58; Article 12]: PETs can help deliver a clear and transparent information to data subjects.
- respect for the data subject's rights provided by the GDPR [Recitals 58-73, 91; Articles 12-22]: PETs can assist data subjects exercising their rights (right to access, right to rectification etc.) [see, i.e. AMI (Access My Info)[27]].

Moreover, PETs are constantly evolving, and new technologies are continuously appearing. This means that when adopting a specific set of PETs, organisations should follow the state-of-the-art criteria in order to ensure data protection compliance.

b. Data breach notification. Article 33 of the GDPR requires controllers to report personal data security breaches which are likely to result in a risk to the rights and freedoms of data subjects to the competent supervisory authority [Article 4 no. 12 of the GDPR defines a personal data breach as a "*breach of security leading to the accidental or unlawful destruction, loss, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed*"].

The GDPR introduces several procedural rules in relation to the notification requirements. The data controller has to **report the breach** to the Authority without undue delay and, where feasible, not later than 72 hours after becoming aware of it (directly or in accordance with processor reporting). Controllers are exempted from notifying a personal data breach to the Data Protection Authority if they are able to demonstrate that the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller has to communicate this event also to the data subject [**Article 34]**. The controller may omit notifying the data subject if, amongst other things, it has implemented appropriate technical and organisational measures in order to protect the data subject's personal data or it has taken subsequent measures which ensure that any high risk to the rights and freedoms of the data subject is no longer expected to materialise.

Failure to report a breach to either the supervisory authority or data subjects, as well as the other requirements of Articles 33 and 34 not being fulfilled (i.e. if the controller fails to act in a timely manner and it becomes apparent that a breach did occur), can lead to fines imposed by the competent supervisory

[26] For further references see, Cranium Campus, *Summary of Privacy Enhancing Technologies – A Survey of Tools and Techniques*, fn. 25.

[27] Access My Info (AMI) is a web application that helps people to create justified requests for copies of their personal information from service providers. For further information see: https://openeffect.ca/access-my-info/, last access 28 September 2019.

authority. The administrative fine value can be up to 10,000,000 EUR or, in the case of a company, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher [Article 83(4)(a)].

c. DPIA. Article 35 of the GDPR imposes that data controllers carry out a Data Protection Impact Assessment (DPIA) prior to the processing of personal data, when the processing is likely to result in a high risk to the rights and freedoms of data subjects. In these cases, the controller is therefore required to assess the impact of the envisaged processing on data subjects' rights and freedoms, taking into account the nature, scope, context and purposes of the processing.

According to the GDPR, a DPIA is a process designed to analyse data processing, assess its necessity and proportionality, identify the risks concerning data processing in terms of negative impacts on the rights and freedoms of natural persons, and take the appropriate measures to address these risks [Articles 35(7); see also Recitals 84 and 90][28].

The DPIA should therefore be seen as a tool for helping decision-making and design strategy concerning data processing, including the choice of the appropriate security measures to put into place to ensure the protection of personal data and safeguard the rights and freedoms of natural persons.

The GDPR provides some cases where a DPIA must be conducted. In addition, the GDPR requires the supervisory authorities to publish a list of activities in relation to which a DPIA must be carried out.

Non-compliance with DPIA requirements (failure to carry out a DPIA when it is compulsory; carrying out a DPIA in an incorrect way or failing to consult the authority where required) can lead to fines imposed by the competent supervisory authority. This infringement can result in an administrative fine of up to 10,000,000 EUR, or in the case of a company, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher [Article 83(4)(a)].

Risk "to the rights and freedoms of individuals"
As indicated by the Article 29 Data Protection Working Party, the reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion[29].

[28] See also 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*", fn. 18.
[29] See, 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*", 6, fn. 18; Article 29 Data Protection Working Party, *Statement on the role of a risk-based approach in data protection legal frameworks*, adopted on 30 May 2014, WP218, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf, last access 2 September 2019, 4.

Cases in which DPIA is required
The GDPR does not require a DPIA to be carried out for every processing operation which may result in risks for the rights and freedoms of natural persons. The carrying out of a DPIA is only mandatory where processing is "*likely to result in a high risk to the rights and freedoms of natural persons*" [Article 35(1); see also Articles 35(3) and 35(4)]. Article 35(3) provides some examples when a processing operation is "*likely to result in high risks*": • "*(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;* • *(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or* • *(c) a systematic monitoring of a publicly accessible area on a large scale*". A list of further criteria to identify processing operations that require a DPIA, due to their inherent high risk, have been provided by the Article 29 Working Party (WP29) (such criteria relate, *inter alia*, to: "*Automated-decision making with legal or similar significant effect*"; "*Systematic monitoring*"; *"Data processed on a large scale*")[30] and, at national level, by Supervisory Authorities.

d. Prior consultation. Where the outcome of the DPIA indicates that the processing involves a high risk, which cannot be mitigated by the controller, the national supervisory authority should be consulted prior to the commencement of the processing (**Art. 36**). In these cases, the authority verifies whether the controller has correctly assessed the risks and taken the adequate measures to tackle or mitigate it, in order to safeguard the rights and freedoms of data subjects.

2.3 Security techniques in the GDPR

As already mentioned, in order to ensure 'appropriate' data protection to individuals, the GDPR requires controllers and processors to adopt all technical and organisational measures, including security measures, that are appropriate to the risk. In this perspective, security measures should cover various aspects of organisation and of data processing, as well as should involve different organisational and technical solutions.

a. Access control and database/network security

Relevant provisions of the GDPR: Recital 39; Article 5 (1)(f); Article 25; Article 32 (1)(b) and (4).

[30] See, 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*", 9, fn. 18.

First of all, in order to protect personal data and, in particular, to ensure their confidentiality and integrity, it is essential to implement an adequate access control policy and system. Controllers should consider the protection against unauthorised access to the system used for the processing of personal data and limit employees and users' access to what is strictly necessary.

From an organisational perspective, access to personal data must therefore be restricted to only those who have a legitimate reason to process or use it.[31] Moreover, each role should only have the level of access to personal data that is strictly necessary for the performance of its relevant tasks.

Security policy

The **security policy** is a document that sets the basic measures for the security and the protection of personal data within an organization.

From an organisational perspective, this document should, in particular, define:

- ***personnel roles and responsibilities***
- ***access control policy***
- ***confidentiality and training of personnel***
- ***resource management***

  The proper management of hardware, software and network resources (e.g. the registration of IoT resources and network topology) is essential for the security of personal data, as it allows to control the adopted organizational and technical measures[32].

- ***incident response plan and business continuity***[33]

These organisational measures should be implemented with the technical ones. In particular, it is important to adopt applications that allow creating, approving, reviewing and deleting user accounts[34]. The use of log files is also an essential security measure, as it enables identification and tracking of user actions; this help to identify potential internal and external attempts for system violation.

The Regulation does not stipulate a specific set of measures to this purpose, but many technologies exist for controlling access, also in relation to network resources. This is the case of, *inter alia*, servers known as

[31] Some examples can be found in: ENISA, *Handbook on Security of Personal Data Processing*, December 2017, https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing, last access 30 September 2019, 34.
[32] See ENISA, *Guidelines for SMEs on the security of personal data processing*, 35, fn. 19.
[33] See below in this Section.
[34] See ENISA, *Guidelines for SMEs on the security of personal data processing*, 40, fn. 19, which, among the different requirements that safety systems should have, highlights "the ability to detect and not allow the usage of passwords that don't respect a certain (configurable) level of complexity".

"Domain Controllers", which normally use a management database to handle authentication for users to machines and services[35].

Moreover, in order to prevent data loss, destruction or damage, it is important to ensure **server and data base security**, as well as **network and communication security**.

In this perspective, several measures could be taken. For instance, controllers should use anti-virus protection and malware detection systems as well as limit wireless access to the IT system. Monitoring traffic to and from the IT system is also important (e.g. through the use of "Firewalls" and "Intrusion Detection Systems"[36]).

The physical security of systems should also be taken into account to ensure a secure operative environment (in this context, controllers should consider, *inter alia*: ID Badges, both for personnel and visitors accessing the premises of the organization; physical barriers; automatic fire suppression systems; continuous power supply; etc.[37]).

b. Data minimisation and techniques to exclude immediate data subject's identification

Relevant provisions: Recitals 28, 39, 83, Articles 5 (1)(c) and (e), 25 (1), 32 (1) (a).

In order to ensure data confidentiality, the GDPR expressly refers to a specific measure that can be adopted from the very initial stage of system design: data minimisation.

From a cybersecurity perspective, a strategy focused on data minimisation can contribute to reduce the impact of data breaches resulting from cyber-attacks or incidents.[38] Controllers should therefore design systems and services in a way that minimises the collection and use of personal data (e.g. websites that not collect and store personal information, such as the search of IP addresses; specific configuration settings in order to prevent personal data processing for purposes different from the original ones).

Moreover, controllers should define the relevant data retention period and adopt systems for automatic deletion of data after the defined period (data storage limitation).

Hiding personal data and their interrelationships from plain view may also be useful for preventing these data to be acquired and misused by unauthorised actors. In this perspective, among the measures that can be taken, the GDPR explicitly indicates pseudonymisation and encryption techniques.

---

[35] See, DQM GRC confidence in data, *Essential Security Technologies for GDPR. Compliance*, available at https://www.dqmgrc.com/file/785/download?token=KuAoDE6C , last access 5 December 2019.
[36] See ENISA, *Guidelines for SMEs on the security of personal data processing*, 41, fn. 19.
[37] See, ENISA, *Guidelines for SMEs on the security of personal data processing*, 46, fn. 19
[38] See also Mantelero, A., Vaciago, G. 2017. Legal Aspects of Information Science, Data Science and Big Data. In Dehmer, M., Emmert-Streib, F. (eds). Frontiers in Data Science. (CRC Press).

However, according to the GDPR, pseudonymisation and encryption techniques are just a few examples of the measures that can be adopted by data controllers and processors to ensure data confidentiality[39].

Pseudonymisation and encryption techniques
Pseudonymisation is defined in Article 4, no. 5, of the GDPR as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person". Other technical definitions of pseudonymisation have been provided by different authorities and standard bodies (e.g. see ISO/TS 25237:2017 and ISO/IEC 20889:2018 standards). There are several techniques that may be utilised for pseudonymisation, such as hashing, hashing with key or salt, encryption, tokenization, as well as other relevant approaches[40]. However, not all pseudonymisation techniques are equally effective, as they do not offer the same level of protection for personal data. It is necessary, therefore, to verify existing solutions and choose the most adequate, considering the protection needs in relation to the specific data processing. Pseudonymisation can support data protection and data security in different ways[41]. To start with the first benefit of pseudonymisation is to hide the identity of data subjects in the context of a specific data processing operation, thus enhancing their security and protection. This is particularly relevant in case, for example, of personal data breaches, where pseudonymisation increases the level of difficulty for a third party to link the breached data with certain individuals. In addition, recognizing the aforementioned properties of pseudonymisation, the GDPR provides a certain 'relaxation' of the data protection obligations if the data controller is able to demonstrate that this technique is applied to processed data. In this sense, personal data can also be further processed for archiving different purposes in the public interest, as well as for different scientific or historical research purposes, when data controllers adopt specific safeguards, such as pseudonymisation [Articles 5 (1)(b) and 89 (1) GDPR]. Moreover, articles from 15 to 20 (i.e. the data subjects rights concerning access to data, rectification and erasure of data) do not apply whenever the controller is unable to identify the users [Articles 11 (2) and 12 (2)].

[39] See RM Long W., Scali G., Blythe F., Raul A. C., *European union overview*, in *Privacy, Data Protection and Cybersecurity law Review*, 2018, 5th edition.

[40] See, ENISA, *Recommendations on shaping technology according to GDPR provisions. An overview on data pseudonymisation*, November 2018, available at https://www.aepd.es/media/docs/recomendations-on-shaping-technology-according-to-GDPR-provisions-2.pdf, last access 5 September 2019. See also Article 29 Data protection Working Party, *Opinion 5/2014 on Anonymisation Techniques*, WP216, adopted on 10 April 2014, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm, last access 5 September 2019.

[41] See, ENISA, *Recommendations on shaping technology according to GDPR provisions. An overview on data pseudonymisation*, 17.

Unlike pseudonymisation, **encryption** aims at ensuring that data is intelligible to anyone but specifically authorised users, who are allowed to reverse this unintelligibility (e.g. to decrypt)[42]. In most cases, data encryption translates data into another form, or code, so that only people with access to a secret key or password can read it.

c. Vulnerability and penetration testing

Relevant provisions: Article 32 (1)(d)

Among the technical and organisational measures that shall be put in place to ensure the protection of personal data, the GDPR also suggests the adoption of testing tools and services to allow controllers and processors to verify the effectiveness of the adopted security technologies. In this sense, during data processing vulnerability assessment, application and infrastructure penetration testing should be performed.

Although the GDPR does not stipulate a specific set of techniques to this purpose, examples of testing tools and services may include, *inter alia*: software to test connections to outside networks and look for gaps in configuration (vulnerability scanning) and ethical hacking (also called "white hat" hacking)[43].

d. Backup techniques and recovery procedures

Relevant provisions: Article 32 (1)(c)

As a part of data security obligations for data controllers and processors, the GDPR requires the adoption of measures that ensure data availability and recovery in case of loss or destruction resulting from a data breach. In this sense, controllers should adopt, for instance, backup techniques and data restore procedures to ensure data availability and access in case of data breach.

e. Resilience of processing systems

Relevant provision: Article 32 (1) (b)

The GDPR also requires controllers to have the ability to ensure the resilience of the processing systems and services. Resilience refers to the ability of the system to continue operating under adverse conditions, such as those that may result from a physical or technical incident and to the ability to restore such systems to an effective state.

[42] Anyway, encryption may also be used as a pseudonymisation techniques, see ENISA, *Recommendations on shaping technology according to GDPR provisions. An overview on data pseudonymisation*, 18.
[43] See, DMQ GRC confidence in data, *Essential Security Technologies for GDPR. Compliance*, 11, fn. 34.

Controllers should therefore take measures to ensure this requirement like the adoption of a "disaster recovery" plan and of an effective "cyber resilience" approach[44]. Moreover, from a technological perspective, controllers should adopt appropriate systems and techniques to ensure business continuity, such as "redundancy techniques".

f. Personal data breaches: Incident response and business continuity

Recitals 85-88; Articles 33 and 34 of the GDPR.

As already mentioned, in the event of a data security breach which is likely to result in a risk to the rights and freedoms of natural persons, the GDPR requires controllers to notify without undue delay the event to the competent supervisory authority and to, amongst other things, "*describe the measures taken or proposed to be taken […]to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects*" [Article 33].

Moreover, the GDPR provides for exceptions to the obligation to communicate a personal data breach to the data subjects [Article 34]. For instance, the controller is exempted from this notification when has "*implemented appropriate technical and organisational protection measures"* that "*render the data unintelligible to any person who is not authorised to access it, such as encryption*" [Art. 34 (3)(a)].

In this regard, in order to avoid any sanctions [see Article 83(4)(a)], controllers should have appropriate technical and organisational measures, not only to prevent a personal data breach or to promptly detect it when it occurs [see Recital 87], but also for the overall handling and management of such events.

This, therefore, requires controllers to have internal processes in place that are able to **detect and address personal data breaches**. Examples of such measures include data flow and log analysers to detect any irregularities in processing of personal data[45]. The GDPR also suggests the adoption of the right tools and technologies which may **limit the consequences of data breaches** and, consequently, also limit notification obligations (e.g. tokenization and encryption[46]). From an organisational perspective, controllers should also establish and document the main procedures to be followed in the event of personal data breaches. This will help the overall handling of such events.

Moreover, controllers must establish an internal register of incidents and personal data breaches (regardless of whether they are required to notify or not the Supervisory Authority according to Article 33), with details

---

[44] See, It Governance, Green paper, *Cybersecurity and business resilience*, available at https://www.itgovernance.co.uk/cyber-resilience, last access 2 September 2019.

[45] See, Article 29, Data Protection Working Party, *Guidelines on Personal data breach notification under Regulation 2016/679*, adopted on 3 October 2017, as last revised and adopted on 6 February 2018, WP250rev.01, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052, last access 2 September 2019, 12.

[46] It should be noted that, even where data is encrypted, a loss or alteration can have negative consequences for data subjects if the controller has not implemented adequate backup procedures. Moreover, when backup procedures exist, the data breach could still have to be notified, depending on the length of time taken to restore the data from backup copies and the effect that lack of availability has on individuals. See, Article 29, Data Protection Working Party, *Guidelines on Personal data breach notification under Regulation 2016/679*, 18, fn. 44.

regarding the event and subsequent mitigation action performed [**Article 33 (5)]**. This documentation could help controllers to demonstrate accountability and compliance with GDPR provisions.

Incident response and business continuity plans
An **incident response plan** with detailed procedures should be define by organizations to ensure effective and immediate response in the event of personal data breach. This plan should contain at least: notification procedures for the reporting of the breaches to competent authorities and data subjects; a list of possible mitigation actions and clear assignment of roles. A **business continuity plan (BCP)** is also essential for determining the main procedures and technical measures to be followed in order to ensure the required level of continuity and availability of the processing data system in the event of personal data breaches or incidents.

2.4 Summary of security obligations in the GDPR

GDPR provides a set of security obligations concerning the protection of personal data which, directly or indirectly, underpin the development of cybersecurity research. This concerns a wide range of security applications that can be grouped into ten main areas, based on their correlation with GDPR principles. The following table shows this correlation between data protection principles, GDPR provisions and the technical and organisational measures that implement, or require the adoption of, cybersecurity techniques.

Table 1: GDPR

Rules and principles	**GDPR**	**Technical and organisational measures**
Data minimization	Recital 39 Article 5.1.c Article 25.1	**Organisational measures** • Identification of data strictly necessary for processing purposes **Technical measures** • Systems and services that minimise data collection and use of personal data
Data storage limitation	Recital 39 Article 5.1.e	**Organisational measures** • Definition of relevant data retention periods **Technical measures**

		• Systems for automatic periodic data deletion
Data confidentiality	Recitals 28, 39, 83 Article 5.1.c and 5.1.f Article 25 Article 32.1a, 32.1.b, and 32.1.4	**Organisational measures** • Security policy (i.e. access control policy; personnel roles and responsibilities; confidentiality and training of personnel; resource management) • Records of processing activities **Technical measures** • Hiding personal data and their relationships (e.g. pseudonymisation and encryption) • Access control to data base and services (applications that allow creating, approving, reviewing and deleting user accounts; log files, etc.) • Server and data base security/network and communication security (e.g. anti-virus protection; malware protection systems; monitoring traffic to and from the IT system) • System's physical security (e.g. Id badges, physical barriers; uninterruptible power supply)
Risk assessment and security measures	Recitals 84 and 90 Article 35	**Organisational measures** • Risk analysis and DPIA, including technical and organisational measures
Data protection by design and by default	Recital 78 Article 25	**Organisational measures** • Adoption of specific security requirements and procedures since the early stages of the development lifecycle • Procedures to integrate data protection safeguards into processing activities

		Technical measures • Specific technologies able to support privacy and data protection (PETs) (i.e. technologies that help to respect, amongst other things, data minimisation, anonymisation or limitation of use principles)
Regular assessment of the effectiveness of the security measures adopted	Article 32.1.d	**Organisational measures** • Records of the adopted technical and organisational security measures **Technical measures** • Vulnerability and penetration testing (e.g. vulnerability scanning; ethical hacking)
Notifications, reporting obligations, and mitigation measures **(data breaches)**	Recital 85, 86, 87 Articles 33, 34	**Organisational measures** • Appropriate procedures to establish immediately whether a personal data breach has taken place • Incident response plan **Technical measures** • Data flow and log analysers • Tokenization; encryption, etc.
Business Continuity, Disaster Recovery, and Resilience	Article 32.1.b and 32.1.c	**Organisational measures** • Business continuity plan • Data restore procedures • Adoption of an effective "cyber resilience" approach • Disaster recovery plan **Technical measures** • Backup techniques • Technological measures to ensure business continuity (e.g. redundancy techniques)

3 The Payment Services Directive framework

3.1 Introduction

On 13 March 2018 the Payment Services Directive (PSD2) was published in the Official Journal of the European Union. Directive (EU) 2015/2366 of the European Parliament and of the Council was released twenty months after the European Banking Authority (EBA) issued the first draft.

It is fully enforceable from 14 September 2019, but since 14 March 2019, Account Servicing Payment Service Providers (ASPSPs) have been under the obligation to make the technical specifications of their APIs (Application Program Interfaces) – be they dedicated or user-facing – available to Third Party Providers (TPPs), and also to provide them with a testing environment to perform integration tests for software programmes and applications that TPPs plan to use to offer services to their users.

The EU's goal of this new regulation is, on one hand, to provide advantages to consumers by stirring up the competition between Account Servicing Payment Service Provider (ASPSPs) and, o the other, to provide a strong harmonised legal framework across the Union.

In brief, PSD2 enables bank customers, both consumers and businesses, to use third-party providers to manage their finances. In the near future, people may be using Facebook or Google to pay their bills, making P2P transfers and analysing their spending, while still having money safely placed in their bank account.

However, according to this regulation, banks must provide these third-party providers access to their customers' accounts through open APIs (application program interface). This will enable third parties to build financial services on top of banks' data and infrastructure.

This Directive represents an upgrade of the existing framework, because it introduces some important new rules with reference to: (i) Positive Scope (ii) Negative Scope (iii) Third-Party Providers (iv) Fees and Surcharges (v) Security (vi) Responsibility.

More in detail:

(i) The Positive Scope is the extension of the application of the transparency rules provided for conditions and information requirements with reference to:

1) payment transactions in a currency that is not that of a Member State, where the payment service provider of the payer and the payment service provider of the payee are both located in the EU-area, or where the sole payment service provider involved in the payment transaction is located within the European territory; only the parts of the payment transaction carried out in the Union fall within the scope of this Directive;
2) payment transactions in all currencies where only one of the payment service providers is located in EU ("one leg"). This is applicable only to those segments of payment transactions carried out within the Union.

(ii) The Negative Scope is the review of existing exemptions pertaining to:

1) Commercial agents: the exemption will only apply to commercial agents involved in the transaction act in favour of only one of the two parties (payer or payee) and not for both;
2) Telecommunications: exemptions applied only to payment transactions made through a provider of electronic communications services or networks for a subscriber to the service or network (e.g. telecommunications operators): (i) to purchase digital content and technological services; or (ii) made by or through an electronic device and charged through the bill as part of a charitable activity or to purchase tickets; in both cases the value of the individual payment transaction must not exceed 50 euros, while the total value of payment transactions for a single subscriber shouldn't be over 300 euros;
3) "Limited network": specified in a more precise manner the notion of networks, to counteract the excessive marketability of this exemption;
4) Independent cash machines (ATM): repealed the exemption included in PSD excluding from the scope of the directive cash withdrawals through ATMs of independent providers ("Independent ATM Deployers").

(iii) The Directive provides the introduction of the "Third-Party Providers" which are new payment services, specifically:

1) Payment Initiation Services (or PISP): a middle layer of services provided to payers accessing their online payment account, managing the payment to a third-party beneficiary. The payer can then make an online payment by direct debit on its account; the PISP must not come into possession of funds from the payer and the payment service provider where the payers' or ASPSP account is held shall grant the PISP access to the online account of the payer;
2) Account Information Service (or AISP): service made available to users of payment services with online access to accounts through which the payer can get, thanks to an online platform, a consolidated view on all its payment accounts, even if those are held on multiple PSP; the AISP cannot use customer data or log on to its payment accounts for any purpose other than providing the service to customers.

(iv) with reference to fees and surcharges the following principles shall be applied and enforced:

1) The SHA principle: the payer and beneficiary each support the fees charged by their respective payment services provider ("SHARE") also to all operations in extra-EU currencies and operations in EU-currencies that involve conversion;
2) A ban on "surcharge" (additional fee) should payment cards be used as provided by EU regulation 2015/751 ("Regulation MIF"), both for domestic and cross-border payments .

(v) The directive provides two different tools in order to provide a safer environment for the financial ecosystem:

1) Fund checking: a new method of checking the availability of funds, which is offered to payment service providers based on card other than ASPSP, to receive confirmation of the availability of funds in case of a payment transaction request by the payer through online platforms that use card-based payment tools. The reply is merely the confirmation or denial of the existence of the funds required to complete the transaction, without any further information.

2) The establishment to ensure the transparency of the functioning of payment institutions, held at the European Banking Authority "EBA", which contains all information relating to the payment institutions associated to individual national Registers. Furthermore, EBA, free-of-charge, will make records available on its website, while, in turn, national authorities will be required to notify the EBA, immediately, any information registered in their respective national registers (for which they remain responsible to guarantee the accuracy) in order to keep the Central Electronic Register updated.

(vi) The concept of responsibility, and specifically the sharing of responsibility between all the parties involved represents a fundamental point which could be identified as the most important improvement enacted through PSD2, extending the scope of the new Directive to PISP and AISP.

It should be duly stressed that - according to the PSD2, - providing a payment initiation service (or an account information service) does not depend on an existent contractual relationship between the PISP/AISP and the payment service provider where the account is held (ASPSP).

This (non-)requirement, together with the provisions of Article 73 (2) of the new Directive,[47] introduce the sensitive issue of responsibilities-sharing between payment service providers. While it is true that these rules introduce a cause of action for ASPSP against the PISP, where the latter is responsible for an unauthorized payment transaction,[48] the absence of a contractual relationship could make the actual enforcement of that provision more difficult.

In conclusion, PSD2 introduces substantial economic challenges for the banking market. IT costs are expected to increase due to new, strong security requirements and the opening of APIs. This – in addition to changed customer expectation and increased digitalization – could be the reason why we see banks experimenting with their APIs, in collaboration with financial technology companies (also known as FinTechs), and focusing on customer centricity and security.

The implementation of PSD2 requires banks to make several strategic choices as far as cybersecurity is concerned. This is not an easy task, as these choices partially depend on how the payment-services business is going to evolve after the PSD2, and this is a change which is largely in progress.

This new framework is based on two variables: 1) the way this new regulation gives the possibility to transfer consumers' personal data, and 2) cybersecurity requirements.

In the following sections, we will take a closer look at these variables, discussing the state of the art and how the scenario might change in the future.

[47] This provision stipulates that, in the event that an unauthorized payment transaction is placed through PISP, the ASPSP will be expected to refund immediately prima facie, and in any case by the end of the next business day, the payer of the amount of the unlawful payment transaction.
[48] On this point see also Article 92 (1), PSD2.

3.2 Preliminary key-points of potential data protection issues

First of all, there are some crucial recitals of this innovative directive which highlight the brand-new approach to cybersecurity adopted by Eu legislator in the context of the digital payments market. In this regard, we have to consider this first part of the directive as an introduction clarifying the overall scope of the entire regulation.

Recitals 4 and 7 basically provide the reason of this review of the EU legal framework on payment services: the previous regulation has resulted in legal uncertainty, potential security risks in the payment chain and a lack of consumer protection in certain areas.

The previous framework has proven difficult for payment service providers to launch innovative, safe and easy-to-use digital payment services and to provide consumers and retailers with effective, convenient and secure payment methods in the EU.

Interconnectedness between corporate/enterprise information technologies is a major challenge related to managing cybersecurity in the financial business. As digitalization increases the number of internet connections, the likelihood of being attacked grows.

This leads to a different approach in which data protection becomes the focus. This approach is fundamental to set right priorities, goals for the maintenance and improvement of technological systems, as well as to define organizational structures and models and policies, which should be carefully drafted and then enforced in order to avoid cultural differences and lack of communication between departments, which in turn could exacerbate cybersecurity problems.

Recital 29 deals with several legal issues, such as consumer protection, security and liability as well as competition and data protection. With specific reference to the protection of users' data related to payment service, the directive dictates that national regulations must to be in accordance with EU data protection rules, i.e., the General Data Protection Regulation.

Consistently with the nature of the adopted instrument, the Directive demands national implementation laws to specifically address all those issues.

Regarding cybersecurity, these provisions show two different aspects. First, the necessity of a national implementation of the European rules in order to customize the European regulation in different national business environments and corporate cultures. Secondly, the importance to have process of information sharing between national and international authorities, aimed at providing guidance on the defensive technology development in the field of cybercrime and related issues, drawing attention to key points for decision makers, manufacturers and service providers.

Specifically, considering that cyber-attacks are a viral phenomenon, authorities are to measure the impact of cybercrime on business communities. National provisions, as well as guidelines and the promotion and introduction of best practices will further contribute to give momentum to the EU security framework in the field of payment services, facilitating the implementation of common cybersecurity strategies across different government bodies and private sector entities.

Attacks and Incidents

When analyzing the number of attacks or incidents that companies have experienced, it is worth noting that a subset of respondents still do not know the number of incidents they have experienced.

In a recent study, about 40% of companies surveyed stated that they have not experienced any cyber-incidents within the last 12 months, which is lower than the 51% recorded last year. While this appears to be a negative development, it is possible these companies simply were unable to identify all incidents in 2018. The higher use of intrusion detection solutions today may expose more cyber-incidents than were visible in the past.

Taking a closer look at the incidents that have occurred, ransomware attacks are the greatest concern. In the 2018, the greatest concern was malware or viruses. Advanced persistent threats (APTs) were recognized as the third greatest concern. The nature of cyberattacks are changing from undirected attacks to targeted attacks that expose companies to 'loss of control' or 'manipulation of control'.[49]

Human factor

The human factor has been defined as all the aspects of personality traits or cognitive factors that can be exploited to influence cybersecurity practices and behaviours. The background against which this exploration is framed is related to insider threats, more specifically those that have no specific motive or malicious intent. Actually, employees can increase cybersecurity-risks, because staff may make mistakes that put company data or systems at risk. This is due to two main reasons: employees are careless, or they do not have the required training about best practices and guidelines to protect the business they work for.[50]

Other challenges for cybersecurity are related to the nature of the human factor. Many security managers have noticed that six to nine months after a successful security awareness training course, employees fall back into their old, dangerous patterns of behaviour. To counter this phenomenon, companies should hold security awareness training courses on a regular basis. [51]

PSD2 provides that data protection by design and data protection by default (see Section 1) should be embedded in all data processing systems developed and used within the framework of this Directive (recitals 99).

[49] Menze, T. 2019. The State of Industrial Cybersecurity. Available at https://ics.kaspersky.com/media/2019_Kaspersky_ARC_ICS_report.pdf.
[50] Hadlington, L. 2018. The "Human Factor" in Cybersecurity: Exploring the Accidental Insider. In McAlaney, J., Anne Frumkin, L., Benson, V. *Psychological and behavioral examinations in cyber security*. Hershey, PA IGI Global.
[51] Menze, fn. 48.

This means that the regulation focused on the importance of technology supporting cybersecurity efforts as a priority, which should then be followed by securing the "human factor" in the cybersecurity scenario. This includes investigating and managing potential links between psychology traits such as impulsivity, decision-making and conscientiousness on one side and information security on the other.

Some of the key techniques and frameworks that can change this behavior and to reach the goal of privacy-designed and privacy-default technologies may not be enough and , therefore, it is also fundamental to consider usability and users' awareness. From a usability perspective it is noted that, for the most part, security protocols and systems are either too confusing or too difficult for the average end-user to engage in effectively (Whitten & Tygar, 1998; Sasse & Flechais, 2005).[52]

This all requires that people need to be trained to use technology and to implement cybersecurity standards, which require a specific organization of the business, often provided by regulations, standards and guidelines.

People Process Technology

Another important model focused on the importance of human behaviour in using technology, is the *People Process Technology*. This is a holistic model for process improvement, which is known and used in several fields. PPT was introduced on a large scale about thirty years ago and is still used as is, without major changes.[53]

Even if, at the beginning, the model was considered applicable only for software development, currently it is applied to any labour-intensive activity which involves people using technology.

According to PPT, people and process must be considered for a holistic perspective. The people part of the equation represents the user needs: these are the ultimate consumers of business intelligence solutions. People, however, are ineffective in their application of business intelligence data and solutions if the processes are not in place to support data-driven decisions. Processes refer to business goals that must be considered to help drive successful changes in business.

People, process and technology must be in alignment for a business intelligence solution to be effective and holistic. Despite its strengths, technology alone does not solve problems without people and processes around to support it.[54] This model can play a significant role in the cybersecurity context where a high level of awareness with regard to people and processing technologies is required.

Another crucial key-point is defined at Recital 91 which states that payment service providers are responsible for security measures. Those measures need to be proportionate to the security risks concerned. This is repeated also in Recital 96, which clarifies that the security measures should be compatible with the

[52] Hadlington, fn. 49.
[53] Prodan, M., Prodan, A., Purcarea, A.A. 2015. *Three New Dimensions to People, Process, Technology Improvement Model*. Polytechnic University of Bucharest.
[54] *Everything You Need to Know about the People, Process, Technology Framework* – Smartsheet, available at https://www.smartsheet.com/content/people-process-technology.

level of risk involved in the payment service. Payment service providers should therefore establish a framework to mitigate risks and maintain effective incident management procedures.

Furthermore, a regular reporting mechanism must be established. On one hand, this should lead to ensuring that payment service providers provide the competent authorities, on a regular basis, with an updated assessment of their security risks and the measures that they have taken in response to those risks.

On the other hand, this also ensure that damages to users, other payment service providers or payment systems (e.g. a substantial disruption of a payment system) are kept to a minimum. From this perspective, it is essential that payment service providers be required to report major security incidents without undue delay to the competent authorities. In this regard, a coordination role will be played by EBA.

According to Recital 92, the security incidents reporting obligations should be without prejudice to other incident reporting obligations laid down in other legal acts of the EU and any requirements laid down in this Directive should be aligned with, and proportionate to, the reporting obligations imposed by other EU laws.

This provision is significant for the compliance with GDPR, NIS Directive and eIDAS Regulation, because all of them have further reporting obligations with slightly different purposes that have to be considered.

The entire legal framework of reporting obligations sets best practices for addressing cybersecurity threats that were inferred from studying financial services, including: (1) conducting comprehensive information sharing on current threats, attack vectors and the systems within the enterprise; (2) implementing baseline protections such as patching against known and potential vulnerabilities; (3) designing and testing security incident response and recovery efforts; and (4) enhancing communications and collaboration by engaging in more regular and formalized collaboration within the sector and national and international authorities.

Given the evolving nature of ransomware attacks, national and international agencies are continuously developing recommendations to help businesses respond. Publications provide methods for preventing, investigating and recovering from ransomware attacks and fact sheets also provides insight to help entities assess their potential breach notification obligations in the wake of a ransomware attack.

Finally, Recital 93 provides that the payment initiation service providers and the account information service providers should observe the necessary data protection and security requirements established by, or referred to in, this Directive or included in the regulatory technical standards. Open standards should ensure the interoperability of different technological communication solutions.[55]

The standards should also guarantee that payment initiation service providers and account information service providers communicate with the account servicing payment service provider and with the customers involved in a secure manner.

The security of communication is a key element in the implementation of this new environment for payment services, because the digitalization of payments leads all payment services to work electronically and this

[55] Those standards should also ensure that the account servicing payment service provider is aware to be contacted by a payment initiation service provider or an account information service provider and not by a client.

must be performed a secure manner. For this reason, these technologies have to be able to guarantee user's safe authentication and to reduce, to the maximum extent possible, any risk of fraud (Recital 95).

3.3 Cybersecurity obligations of the PSD2

In PSD2 Directive, there are several provisions that set important obligations for the different entities involved in the payment market environment. The main provisions in this regard are briefly discussed here.

Having regard to *Applications for authorization* (Article 5), payment institutions should meet specific requirements to be granted an authorization to operate. These requirements are enumerated therein, and it is established that an application shall be submitted to the competent authorities of the home Member State.

Accordingly, the PSD2 defines some important requirements regarding cybersecurity, such as:

- A description of the **procedure in place** to monitor, handle and follow up a **security incident** and security related customer complaints, including an incident reporting mechanism which takes account of the notification obligations of the payment institution laid down in Article 96;
- A description of **business continuity arrangements** including a clear identification of the critical operations, effective contingency plans and a procedure to regularly test and review the adequacy and efficiency of such plans.

Both these requirements show not only the importance of communications and the reporting obligations provided by this new regulation, but also the relevance of business continuity and disaster recovery in case of cyber incidents.

These provisions are coherent with the need to implement specific cybersecurity technical standards which requires, on one hand, risk management, security readiness and incident response preparedness in reducing the risks and consequences of major cyber and physical events security readiness, including (1) a proper corporate governance structure; (2) security policies and incident response plans, procedures and toolkits; (3) information sharing arrangements with government agencies and industry centers; (4) table-top exercises; (5) third-party vendor contracts and management; (6) insider threat programs; and (7) employee training programs.

On the other hand, in case of cyber incidents and major physical security emergencies, adopt a comprehensive incident response in managing the full panoply of activities associated with a significant cyber or physical security incident is needed. This includes (1) conducting internal investigations; (2) engaging with law enforcement and regulatory agencies; (3) ensuring compliance with individual notification requirements and government reporting obligations; (4) preparing for litigation and advising on information retention obligations; (5) managing public relations, employee communications and investor relations; (6) managing legislative inquiries and preparing executives for hearings; and (7) handling the ensuing class action lawsuits, government enforcement actions and alternative dispute resolution proceedings.

All these different factors must be included and detailed in the applications for authorizations.

Moreover, Article 94 (Chapter 4) states that Member States also permit processing of personal data by payment systems and payment service providers when necessary **to safeguard the prevention, investigation and detection of payment fraud**. In this case, the provision of information to individuals about the processing of personal data and the processing of such personal data and any other processing of personal data for the purposes of this Directive will be carried out in accordance the data protection regulation.

Furthermore, in line with the purpose specification principle (see above Section I), payment service providers can only access, process and retain personal data necessary for the provision of their payment services with the explicit consent of the payment service user.

Chapter 5 of PSD2 pertains to Operational and security risks and authentication and provides a legislative scheme about Management of operational and security risks (Article 95), Incident reporting (Article 96), Authentication (Article 97) and Regulatory technical standards on authentication and communication (Article 98).

With reference to management of operational and security risks, Article 95 provides that all Member States should guarantee that Payment Service Providers provide a scheme of appropriate mitigation measures and control mechanisms. They must also establish and maintain effective incident management procedures, which should include the detection and classification of major operational and security incidents.

At the same time these providers must forward to the competent authority an updated and comprehensive assessment of the operational and security risks, on an annual basis or at shorter intervals as determined by the competent authority. This requirement is essential in order to prevent incidents and create a correct awareness about current risks.

In conclusion, these different rules require the establishment, implementation and monitoring of the security measures, including certification processes. In this regard, if requested by the Commission, EBA shall develop draft regulatory technical standards on the criteria and on the conditions for establishment, and monitoring of security measures. Moreover, cooperation on this matter is promoted by EBA, including the sharing of information among the competent authorities and between the competent authorities and the ECB and, where relevant, the ENISA.

Comprehensive Security Approach
The analysed provisions advocate a modern comprehensive security concept including: i) cyber-security measures ii) mitigation and control mechanisms iii) effective management and annual report. By analysing these obligations with the model “people process technology”, as already mentioned in the box above, it can be considered a classification as the following. • Technology: cyber-security measures • People: mitigation plan and control mechanism

- Process: certification processes (or effective management) and annual report.

It can also be noticed that these points have to play a role with a different timesheet.

- Technology: security measures => before incidents to prevent it.
- People: mitigation plan and control mechanism => during incident to afford it.
- Process: certification processes (or effective management) and annual report for the future to develop standards.

Regarding **notification obligations**, a major operational or security incident must be notified, without undue delay, by payment service providers to the competent authority in the home Member State of the payment service provider (Article 96). Then if the incident has or may have an impact on the financial interests of its payment service users, the provider must inform its payment service users about the incident and the mitigation measures, without undue delay.

The relevant National Authority notifies the incident to EBA and ECB and, after assessing the relevance of the incident to relevant authorities of that Member State and – should it be necessary - to other local authorities. ECB and EBA, with the notifying national authority, assess the relevance of the incident to other relevant Union and national authorities and will notify them accordingly. The ECB will notify the members of the European System of Central Banks on issues relevant to the payment system.

This scheme of notifications is clearly aimed at allowing the competent authorities to take all the necessary measures to protect the immediate safety of the financial system. National regulations shall require providers to issue an annual report - to be sent to the National Authorities - showing statistical data on frauds.

Finally, EBA will issue specific guidelines with reference to the classification of major incidents and criteria on how to assess the relevance.

Further provisions in the PSD2 Directive concern **authentication systems**. Article 97 requires to Member States to ensure that a payment service provider applies strong customer authentication when the payer interacts with the system in the following cases: (a) access to payment account online; (b) electronic payment transaction; (c) any action carried out through a remote channel which may imply a risk of payment fraud or other abuses.

This is the provision that most emphatically shows how the entire new environment for financial payments must be focused on and then implemented with secure technological measures preventing frauds and unauthorized accesses. In fact, Member States are required to make sure that payment service providers deploy adequate security measures to protect the confidentiality and integrity of payment service users' unique security credentials.

In addition to an increased level of security in the payment services market, PSD2 also aims to enable non-banks players to operate in the business of banking or financial services. This means that both these groups are required to ensure security of data and information processed by technologies.

Secure technologies for financial institutions and non-banks players

The changes introduced by the new Directive are noticeable and require the deployment of modern technology and the development of modern tools of digital transformation, which in tun require advanced secure solutions for processing data and not only for secure payments such as:

- Encryption
- Compliance management
- Public key infrastructure
- Identity verification systems and access control systems
- Privacy requirements and privacy architecture
- Deep packet inspection (DPI)
- Up-to-dated and secure tools for communications
- Personal information classification system capable to take trace of types of incidents and alerting systems
- Set of capabilities to enable both real-time and offline monitoring and dashboarding that support necessary personal information and event correlation and integration
- Set of capabilities to enable both real-time and post-event alerting, reporting and correlation of events, incidents, processes and ticketed actions, as well as support for proper escalation and remediation
- Up-to-dated procedure and standards for isolation of different systems and networks
- Tools for privacy forensics analysis
- Security information and event management
- Log analysers and inspection tools
- Analysis and auditing tools procedures and tools for periodical assessments
- Privacy-friendly user profile settings, for example, limiting from the start the accessibility of the users' profile so that it is not accessible by default to an indefinite number of persons.

With regard to **regulatory technical standards** on authentication and communication as the Directive imposes several obligations on EBA, such as the development of draft regulatory technical standards addressed to payment service providers, specifying: (a) requirements of the strong customer authentication (b) exemptions from the application of the strong authentication (c) requirements security measures have to comply with (d) requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information.

The draft regulatory technical standards shall be developed to ensure the safety of payment service users' funds and personal data, as well as the fairness of the competition among all payment service providers. Further requirements are technology and business-model neutrality, and the development of user-friendly and accessible means of payment.

In conclusion it is also required to EBA to review and, if appropriate, update the regulatory technical standards on a regular basis in order to consider innovation and technological developments.

For example, among duties specifically provided by the Directive, the European Banking Authority's Guideline (2017) sets out the criteria and methodology to be used by payment services to consider an

incident as major and, therefore to be subject to notification to the competent authority in the Member State. Accordingly, the Financial Stability Board (FSB) identifies:

- mitigating operational risk from third-party service providers,
- increasing cyber-security measures, and
- monitoring macro-financial risks

as the three mayor priority areas for international cooperation.

3.4 Summary of security obligations

The Directive provides the introduction of Third-Party Providers (PISP and AISP) which are new payment services having roles which allow them to access to users' accounts. This innovative system requires technologies able to protect financial data in order to prevent insecurity of the whole environment for both banks and non-banks institutions.

Recital 93 underlines the necessity to realize a system in which the regulatory technical standards should be compatible with the different technological solutions available. This particular business model, whether based on direct or indirect access, should observe the necessary data protection and security requirements established by, or referred to in, this Directive or included in the regulatory technical standards.

The new environment provides several channels and communications for all players. Accordingly, the need to study every different kinds of communications - because each type of information-exchange is characterized by different several features – arises.

The main categories of players detailed by the Directive are the following:

- PISP/AISP and banks
- Different Authorities of Member States
- National Authorities and European organizations
- EBA and ECB.
- In conclusion it looks that technologies to be adopted in line with the aforementioned purposes shall be necessarily designed and aimed at preventing unlawful access to data and information shared between different players and between providers and Authorities.

Table 2: PSD2 Directive

Rules and principles	PSD2	Technical and organisational measures
Risk assessment and security measures[56]	Recitals 91 and 96 Article 5.1.j Article 95.1 Article 97	**Organisational measures** • Operational and security risk management framework (consistent, properly documented, updated, implemented and monitored) • Control model, to identify and manage operational and security risks • Risk assessment **Technical measures** • Physical security • Access control (physical and logical access, strong controls over privileged system access) • Continuous monitoring and detection
Data protection (security) by design and by default	Recital 89	**Technical measures** Secure technologies by design and by default should find solutions to common critical points, among which are: • Connectivity into banks • Security fraud and liability • No standards around disputes and complaints • Uncertainty about monetizing data • Poor user authentication experiences • Granting permissions Possible solutions: • Systems capable to eliminate/reduce personal data or prevent unnecessary or undesired processing or derivation of personal data • Implementation of pseudonymization (replacing personally identifiable material with artificial

[56] "*These Guidelines specify requirements for the establishment, implementation and monitoring of the security measures that PSPs must take, in accordance with Article 95(1) of Directive (EU) 2015/2366, to manage the operational and security risks relating to the payment services they provide*" – EBA. Final Report on Guidelines on Security Measures for Operational and Security Risks under PSD2 https://eba.europa.eu/sites/default/documents/files/documents/10180/2060117/d53bf08f-990b-47ba-b36f-15c985064d47/Final%20report%20on%20EBA%20Guidelines%20on%20the%20security%20measures%20for%20operational%20and%20security%20risks%20under%20PSD2%20(EBA-GL-2017-17).pdf

		identifiers) and encryption (encoding messages so only those authorized can read them) • Implementation of users' profiles settings in the most privacy-friendly by, for example, limiting from the start the accessibility of the users' profile so that it isn't accessible by default to an indefinite number of persons (i.e. facial/iris recognition)
Notifications, reporting obligations, and mitigation measures	Article 96 Article 5.1.f	**Organisational measures** • Appropriate processes and organisational structures to ensure the consistent and integrated monitoring, handling and follow-up of operational or security incidents • Procedure for reporting **Technical measures** • Early warning indicators that should serve as an alert to enable early detection of operational or security incidents
Business Continuity, Disaster Recovery and Resilience	Article 5.1.h	**Organisational measures** • Identify a range of different scenarios • Develop response and recovery plans, which should: o Focus on the impact on the operation of critical functions, processes, systems, transactions and interdependencies; o Be documented and made available to the business and support units and readily accessible in case of emergency; o Be updated in line with lessons learned from the tests, new risks identified and threats and changed recovery objectives and priorities o Governance arrangements and crisis communication plans o Procedures to verify the ability of staff and processes to respond adequately to the scenarios above **Technical measures** • Backup techniques

Certification process[57]	Article 95.3	**Organisational measures**
		• The Guidelines do not specify requirements in relation to certification processes, and also, as far as possible, to industry standards such as ISO 27001/22301; given that
		  ○ no national authority requires such certification processes at present
		  ○ the EBA is not mandated to make certification processes compulsory
		  ○ the alternative of market-driven certification processes is voluntary, the EBA has concluded that there is little subject matter that could conceivably be harmonised through EBA Guidelines.
		• The Guidelines therefore stay silent on this particular topic for now, which may change at some point in the future, should the market or regulatory practices change such that the Guidelines need to be amended during the regular reviews that the EBA will carry out.

Annual report to the European Authority [58]	Article 96.6 (report to National Authority which provides to EBA and ECB)	**Organisational measures** • Record data from all agents and aggregate data (geographical perspective, payment channels, authentication method, etc.) • Statistical reporting systems

[57] Source: EBA. Final Report on Guidelines on Security Measures for Operational and Security Risks under PSD2 – https://eba.europa.eu/sites/default/documents/files/documents/10180/2060117/d53bf08f-990b-47ba-b36f-15c985064d47/Final%20report%20on%20EBA%20Guidelines%20on%20the%20security%20measures%20for%20operational%20and%20security%20risks%20under%20PSD2%20(EBA-GL-2017-17).pdf

[58] Source: EBA. Guidelines on fraud reporting under PSD2 https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-fraud-reporting-under-psd2

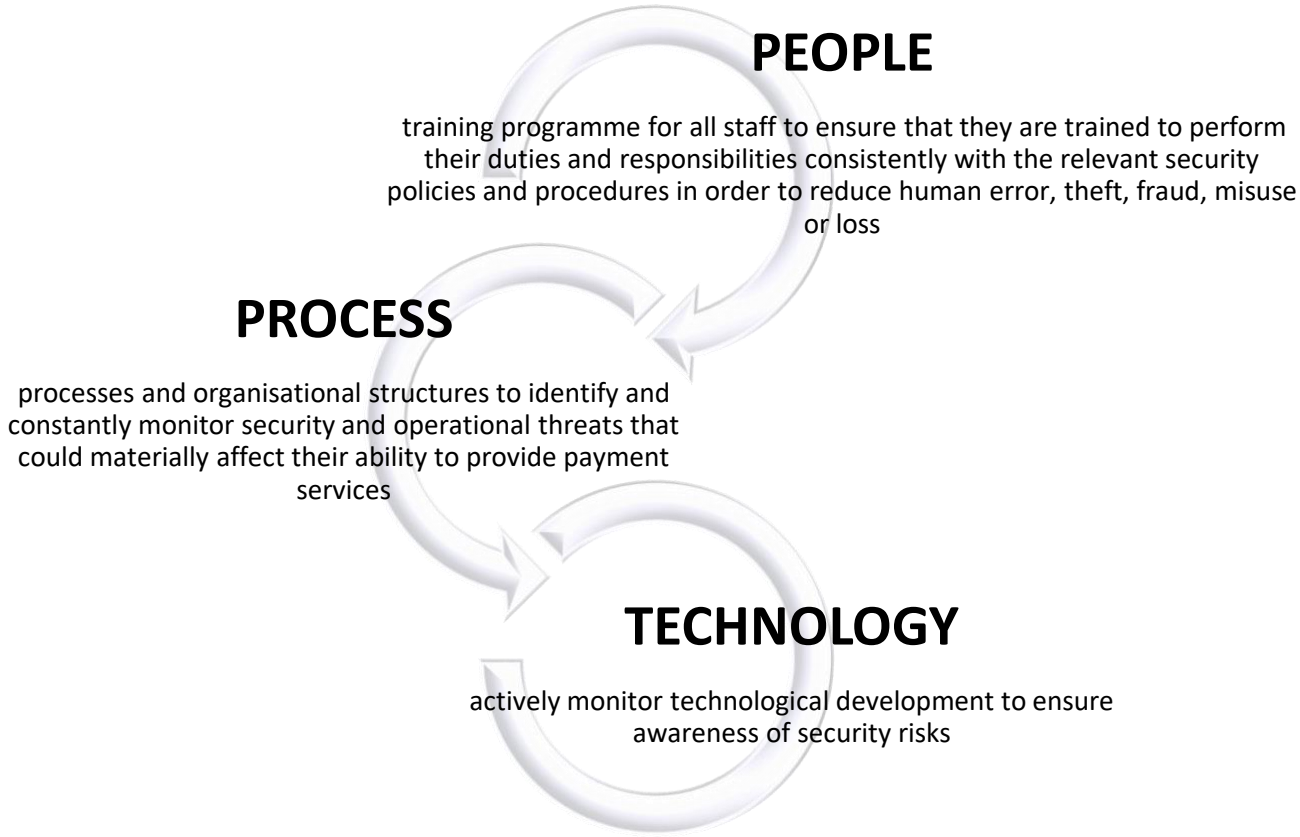

Figure 1: PSD2 Directive

4 The Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) framework

4.1 Introduction

eIDAS Regulation[59] concerns authentication, signature seals, registered delivery services and time stamps. It replaces the former regulation – the eSignature Directive (Directive 1999/93/EC) – which was outdated and suffered from some shortcomings with reference to supervisory duties on national authorities with reference to local service providers.

eIDAS Regulation brought a new layer to Digital Signature Regulation and aims at achieving several key-points:

- Make cross-border electronic transactions more secure and trustworthy
- Foster transparency and standardization in the market
- Ensure accountability
- Facilitate citizens' interaction with Member States' administration through online administration
- Decrease red tape for businesses, meaning overheads can be reduced and profits increased
- Increase flexibility and convenience of government services.
- The regulation replaced the former eSignature Directive and aims to eliminate any current inconsistency in Digital Signature regulations across the EU. It was adopted in July 2014, with regulations for trust services coming into force 1st July 2016. The mandatory mutual recognition of electronic identities (eIDs) is enforceable from mid-2018.
- eIDAS is applicable to any person or business operating in the EU using electronic signatures for identity verification and electronic transactions.
- One of the main innovations introduced is the difference between Advanced Electronic Signatures (AdES) and Qualified Electronic Signatures (QES). These are set in order to provide consistency across all EU member states in the way that Document Signing is carried out.
- Both AdES and QES prove identity of the signer and are the equivalent to an ink signature. The difference is the acceptance by other EU Member States (i.e., states other than where the trust provider originated).
- It is also important to consider that an AdES will have legal effect and admissibility as evidence in legal proceedings solely on the grounds that evidence is in electronic form and it complies with the requirements for qualified electronic signatures.

[59] Regulation (EU) No 910/2014 of the European Parliament and of Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Furthermore, eIDAS also introduces the recognition of electronic seals which are like signatures but can be linked only to legal persons and corporate entities. An electronic seal is data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.[60]

Article 8 of the new regulation establishes three levels of assurance for identification schemes that are directly proportional to their legal value:

- Low Assurance provides limited confidence in the identity of the signer (e.g. this type of credential might only prove ownership of an email address)
- Substantial Assurance provides a limited degree of confidence in the claimed identity of a signer (e.g. to achieve this assurance level it is necessary to prove ownership of an email address and the identity of the signer)
- High Assurance provides a high degree of confidence in the claimed identity of a person. In addition to proving the person's identity, a high assurance credential might also prove legal representation of organization(s) by the individual at hand.

Whatever the assurance level, States who have notified an identity scheme become liable for it, as well as for the registration of data operators, and identity/authentication providers included in the notified scheme.

Moreover, for electronic signatures to pass the eIDAS qualifications they must be created using a Digital Certificate purchased from a 'trust services provider', such as a Certificate Authority (CA). Trust service provider must follow the guidelines set out by eIDAs and comply with the following obligations::

- Verify the identity of attributes of the person whom the certificate will be issued for, by having the person physically present (for low assurance this can be an electronic presence)
- Inform a supervisory body of any changes in the provision of its trust services and any intention to revoke certificates.
- Train staff in data and security best practices.
- Be able to store data and certificates with utmost security and highest forms of trust as well as taking measures to avoid forgery or theft.
- Keep data on certificates for an appropriate period of time, even after a certificate has been revoked. This is recommended to be done in a certificate database where it can register any changes such as revocation.

In the following chapter, these variables shall be thoroughly examined, discussing the current situation and how the scenario might change in the future .

[60] This kind of seal is similar, in its function, to the traditional business stamp and can be applied to an electronic document to guarantee the origin and integrity of a document.

4.2 Preliminary key-points of potential data protection issues

This regulation should be applied in full compliance with the principles relating to the protection of personal data (Recital 11). In this respect, having regard to the principle of mutual recognition established, authentication for an online service should concern processing of only those identification data that are adequate, relevant and not excessive to grant access to that service online. Furthermore, requirements concerning confidentiality and security of processing should be respected by trust service providers and supervisory bodies.

The new rules increased the level of coherence, both across EU institutions (horizontal) and between them and member states (vertical). This can be seen from an institutional perspective, in terms of institutional coordination, but also as a deeper shared understanding of what cybersecurity is and how it should be approached.[61]

In this regard, as already mentioned, the regulation introduces **assurance levels** (Recital 16) that define the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned to.

The assurance level depends on the degree of confidence that electronic identification solutions provide in claimed or asserted identity of a person, taking into account the processes actually adopted (e.g. identity proofing and verification, and authentication), management activities (e.g. the entity issuing electronic identification means, the procedure to issue such means) and technical controls implemented.

Various technical definitions and descriptions of assurance levels exist as the result of EU-funded large-scale pilots projects, of standardization and of international activities. In particular, ISO 29115 refers, *inter alia*, to levels 2, 3 and 4, which should be carefully taken into account in establishing minimum technical requirements, standards and procedures for low, substantial and high assurance levels within the meaning of this Regulation.

The requirements established should be technology-neutral and it should be possible to achieve the necessary security requirements through different technologies.

ISO29115
ISO/IEC 29115, also called *Information technology — Security techniques — Entity authentication assurance framework*, is a standard reviewed every 5 years and provides a framework for managing entity authentication assurance in a given context. In particular, this standard specifies four levels of entity authentication assurance, and the criteria and guidelines for achieving each of the four levels of entity

[61] Barrinha, A., and Farrand-Carrapico, H. 2018. How Coherent is EU cybersecurity policy? in EUROPP – European Polictics and Policy - available at https://blogs.lse.ac.uk/europpblog/2018/01/16/how-coherent-is-eu-cybersecurity-policy.

authentication assurance. It also provides guidance concerning (1) the mapping other authentication assurance schemes regarding the four levels of entity authentication; (2) the exchange of the results of authentication based on these four levels; (3) controls that should be used to mitigate authentication threats.

To facilitate technical interoperability of the notified electronic identification schemes, and with a view to fostering a high level of trust and security appropriate to the degree of risk, **cooperation between Member States** must be implemented (Recital 20). The exchange of information and the sharing of best practices between Member States should help such cooperation.

In this context, the focus on security is crucial and all trust service providers must apply good security practice, appropriate to the risks related to their activities, to boost users' trust.

Secure Channel

A secure channel of communication should be characterised by three main requirements:

- Private: information shouldn't be viewable by any third parties;
- Hard to penetrate: it should be extremely difficult for any cybercriminals to break into an IT system by guessing passwords or credential, exploiting bad code, or leveraging API loopholes;
- Reliable: communication should be consistently reliable, with no interruptions or vulnerabilities to exploit.

An example of a secure form of communication is Microsoft Schannel (Microsoft Secure Channel), which is a security package that facilitates the use of Secure Sockets Layer (SSL) and/or Transport Layer Security (TLS) encryption on Windows platforms.

Schannel contains four specific security protocols that provide identity authentication and private communication between a client and a server, and automatically chooses the best protocol depending on the capabilities of the client and server. The protocols include TLS 1.1 and 1.2, and SSL 2.0 and 3.0.

To create a secure connection, both the client and server need to obtain Schannel credentials (X.509 certificates) and then create a security session. Once the connection is established, information about the attributes of the credential and its context is available. If a connection is lost, it can be renegotiated by requesting a redo. Before shutting down the connection, both client and server need to perform a cleanup and then delete the connection.

Recitals 34, 35 and 36 require a **coherent European system** n which all Member States follow common essential supervision requirements to ensure a comparable security level for all qualified trust services. To ease the consistent application of those requirements across the EU, Member States should adopt comparable procedures and should exchange information on their supervision activities and best practices in the field. In this sense, supervisory regime for all trust service providers should be adopted, to ensure a level playing field for the security and accountability of their operations and services.

The role of EU Institutions

European institutions took important steps in strengthening their cooperation in the fight against cyber-attacks and provide a high level of cybersecurity. Several inter-institutional arrangements established permanent organizations, such as EDPB, ENISA, CERT-EU, etc. in order to:

- Provide an overall coordination between member states
- Ensure the implementation of standards and guidelines
- Adopt practical measures against cybercrimes, such as streamlining mutual legal assistance (MLA) proceedings, cooperation with service providers, launching a reflection process on possible connecting factors for enforcement jurisdiction in cyberspace;
- In case of attack, coordinate responses to stop the attack spread as a viral phenomenon.

Both Recitals 38 and 39 provide specific requirements for incident **notifications**. To enable the Commission and the Member States to assess the effectiveness of the breach notification mechanism introduced by eIDAS, supervisory bodies are requested to provide summary information to the Commission and to European Union Agency for Network and Information Security (ENISA).

In terms of **security standards**, the Regulation (Recital 55) recognizes the role of existing IT security certification based on international standards and expressly mentions ISO 15408. With regard to future standards, evaluation methods and mutual recognition arrangements are important to define those standards, which play a crucial role in verifying the security of qualified electronic signature creation devices. For this reason, the standardization process should be promoted.

ISO 15408

ISO/IEC 15408 (Information technology — Security techniques — Evaluation criteria for IT security) establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.

The standard is made up of three parts:

Part 1 (Introduction and general model) is an introduction to ISO/IEC 15408. It defines general concepts and principles of IT security evaluation and presents a general model of evaluation. Part 1 also presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems. In addition, the usefulness of each part of ISO/IEC 15408 is described in terms of each of the target audiences.

Part 2 (Security functional requirements) establishes a set of functional components as a standard way of expressing the functional requirements for TOEs (Targets Of Evaluation). Part 2 catalogues the set of functional components, families, and classes.

Part 3 (Security assurance requirements) establishes a set of assurance components as a standard way of expressing the assurance requirements for TOEs. Part 3 catalogues the set of assurance components,

families and classes; evaluation criteria for f Protection Profiles (PPs) and Security Targets (STs) are also defined here. Moreover, this part presents evaluation assurance levels that define the predefined ISO/IEC 15408 scale for rating assurance for TOEs, called the Evaluation Assurance Levels (EALs).[62]

This regulation also requires a system of European bodies such as the European Committee for Standardization (CEN), the European Telecommunications Standards Institute (ETSI). This is the only way to ensure security and trust.

In order to ensure a coherent framework and overall a good level of security, the Commission should take due account of the standards and technical specifications drawn up by European and international standardization organizations and bodies when adopting delegated or implementing acts.

European standardization organization

The European standardization organizations (CEN, CENELEC and ETSI) created in 2011 the Cybersecurity Coordination group to provide strategic advice on standardization in the field of IT security, Network and Information Security (NIS) and Cyber Security (CS). The Group was converted into CEN-CENELEC Focus Group on Cybersecurity in 2016.

The Focus Group on Cybersecurity (CSCG) will support CEN and CENELEC to explore ways and means for supporting the growth of the Digital Single market. To this end, the CSCG will analyse technology developments and develop a set of recommendations to its parent bodies for international standards setting ensuring a proper level playing field for businesses and public authorities.

The Group will prepare a European roadmap on cybersecurity standardization and will actively support global initiatives on cybersecurity standards that are compliant with EU requirements in view of development of trustworthy ICT products, systems and services[63].

4.3 Cybersecurity obligations of eIDAS

With a view to ensuring the proper functioning of the internal market while aiming at an adequate level of security of electronic identification means and trust services, eIDAS aims to achieve the following goals:

(a) Lay down the conditions under which Member States recognize electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State

[62] Source: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-standard-15408

[63] https://www.cencenelec.eu/standards/Sectorsold/DefenceSecurityPrivacy/Security/Pages/Cybersecurity.aspx

(b) Lay down rules for trust services, in particular for electronic transactions

(c) Establish a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.

It is important to consider that the regulation allows national legislators to customize the implementation but requires specific criteria in order to ensure a reliable system and build a secure information

To achieve an adequate level of security of electronic identification means and trusted services, Member State shall notify to the Commission the following information:

- A description of the electronic identification scheme, including its assurance levels and the issuer or issuers of electronic identification means under the scheme
- The applicable supervisory regime and information on the liability regime with respect to the party issuing the electronic identification means, and the party operating the authentication procedure
- The authority or authorities responsible for the electronic identification scheme
- Information on the entity or entities which manage the registration of the unique person identification data
- A description of how the requirements set out in the implementing (national) acts referred to in Article 12(8)[64] are met
- A description of the authentication
- Arrangements for suspension or revocation of either the notified electronic identification scheme or authentication or the compromised parts concerned.

The role of European Commission in eIDAS

The European Commission plays a crucial role in the eIDAS regulation because such legislative act represents the basis to improve the European Digital Economy and Society, which is a task of EU Commission.

According to the DESI (Digital Economy and Society Index), released by the Commission every year, Countries that have set up ambitious targets in line with the EU Digital Single Market Strategy and combined them with adapted investment achieved a better performance in a relatively short period of time. However, the fact that the largest EU economies are not digital frontrunners indicates that the speed of digital transformation must increase for the EU to keep on par at world level.[65]

[64] By 18 September 2015, for the purpose of setting uniform conditions for the implementation of the requirement under paragraph 1, the Commission shall, subject to the criteria set out in paragraph 3 and taking into account the results of the cooperation between Member States, adopt implementing acts on the interoperability framework. This interoperability framework shall meet the following criteria: (a) it aims to be technology neutral and does not discriminate between any specific national technical solutions for electronic identification within a Member State; (b) it follows European and international standards, where possible; (c) it facilitates the implementation of the principle of privacy by design; and (d) it ensures that personal data is processed in accordance with data protection rules.

[65] Source: https://europa.eu/rapid/press-release_IP-19-2930_en.htm

In this regard, Commissioner for the Digital Economy and Society, Mariya Gabriel, added: "*This year's Digital Economy and Society Index demonstrates that the speed of digital transformation must accelerate for the EU to stay competitive at world level. In order to succeed, we have to continue to work together for an inclusive digital economy and ensure unimpeded access to digital skills for all EU citizens in order to truly thrive and build a more digital Europe.*"[66]

From this perspective, the coordination of the European Commission is fundamental in this specific field, to improve connectivity and reliability of the digital market.

Article 10 provides requirements in case of **security breach**, particularly the importance of the **notification** to the competent authority and the remediation plan, in order to contain the spread of the breach.

Firstly, where either the electronic identification scheme notified is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme, the notifying Member State shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform other Member States and the Commission.

Secondly, when the breach is remedied, the notifying Member State shall re- establish the cross-border authentication and shall inform other Member States and the Commission without undue delay.

If the breach is not remedied within three months of the suspension or revocation, the notifying Member State shall notify other Member States and the Commission the withdrawal of the electronic identification scheme.

The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list without undue delay.

Risk Assessment

Common types of cyber vulnerabilities and core process can implement and maintain a vulnerability management program in order to decrease cybersecurity risks.

Vulnerabilities are weaknesses or other conditions in an organization that a threat actor, such as a hacker, nation-state, disgruntled employee, or other attacker, can exploit to adversely affect data security. Cyber vulnerabilities typically include a subset of those weaknesses and focus on issues in the IT software, hardware, and systems an organization uses. For example:

- Design, implementation, or other vendor oversights that create defects in commercial IT products
- Poor setup, mismanagement, or other issues in the way an organization installs and maintains its IT hardware and software components (see Unsecured Configurations).

Vulnerabilities can be defined by a risk assessment which allows to target potential vulnerabilities of the IT infrastructure (networks, devices, platforms, etc.) and the organization. A risk assessment is

[66] For more information: https://ec.europa.eu/digital-single-market/desi

fundamental to address these issues. Common vulnerabilities that organizations must also tackle in their information security programs include:

- Gaps in business processes
- Human weaknesses, such as lack of user training and awareness
- Poorly designed access controls or other safeguards
- Physical and environmental issues.

Remediation Plan

Even if theoretically a risk assessment is not required to provide a good remediation plan, this plan is necessary in order to have a map of the used systems and potential leaks of security.

Actually, organizations cannot protect assets unless they know about them. Maintaining a detailed IT hardware and software asset inventory, including specific versions, is a foundational element of any best practice based on information security program.

Organizations typically remediate identified vulnerabilities by:

- Diligently implementing organizational measures in order to mitigate attacks or cyber incidents, such as designing a cyber response team and specific policies
- Applying patches or other vendor-supplied updates for hardware and software
- Updating configurations to use more secure settings or deactivate unnecessary services or communication channels.

Some organizations use automated software distribution tools or other products to apply patches and track software updates, especially those with large or complex IT environments. However, a good remediation plan needs to be implemented with organizational measures, first of all by assigning authority and establishing information security policies to ensure that they acquire, develop, and track IT assets in a secure manner.

Article 12 concerns **cooperation and interoperability**. This article provides that the interoperability framework shall consist of common operational security standards and Member States shall cooperate regarding the security of the electronic identification schemes. In this context, the regulation introduces the role of the Supervisory body, which has to inform other supervisory bodies and the public about breaches of security or loss of integrity (Article 17).

Article 19 provides **security requirements** applicable to trust service providers, specifically technical and organizational measures and notification of breaches. In this regard, qualified and non-qualified trust service providers shall take appropriate technical and organizational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimize the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.

Regarding the **notification obligations**, qualified and non-qualified trust service providers must, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies (e.g. the competent national body for information security or the data protection authority) of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.

Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the notified supervisory body shall inform the supervisory bodies in other Member States concerned and ENISA.

The notified supervisory body must inform the public or require the trust service provider to do so, where it determines that disclosure of the breach of security or loss of integrity is in the public interest. Once a year, the supervisory body shall provide ENISA with a summary of notifications of breach of security and loss of integrity received from trust service providers.

ENISA Threat Landscape
The ENISA Threat Landscape provides an overview of threats, together with current and emerging trends. It is based on publicly available data and provides an independent view on observed threats, threat agents and threat trends. Hundreds of reports from security industry, networks of excellence, standardization bodies and other independent institutes have been analysed. The ENISA Threat Landscape 2018 provides a comprehensive compilation of top 15 cyberthreats encountered within the time period December 2017 - December 2018. 2018 was a year that has brought significant changes in the cyberthreat landscape. Those changes had as source discrete developments in motives and tactics of the most important threat agent groups, namely cyber-criminals and state-sponsored actors. Monetization motives have contributed to the appearance of crypto-miners in the top 15 threats. State-sponsored activities have led to the assumption that there is a shift towards reducing the use of complex malicious software and infrastructures and going towards low profile social engineering attacks. These developments are the subject of this threat landscape report.[67]

[67] Source: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape

4.4 Summary of security obligations

The two main key points about cybersecurity in eIDAS concerns appropriate technical and organizational measures to manage the risks and the notification security incidents.

The regulation requires two different type of notifications. The first is the description of the electronic identification procedures in each Member State. In this regard, the Commission publishes in the Official Journal of the European Union a list of the electronic identification schemes which were notified. The second kind of notification regards cases of security-incidents and it follows the field of the whole recent European regulations.

Furthermore, supervisory body must provide ENISA once a year with a summary of notifications of breach of security and loss of integrity received from trust service providers.

This entire framework underlines the importance of the ENISA-role, because in this matter, among others, it is crucial to monitor the entire cross-border field and activate proactive defenses. Specifically, an internationally oriented guide should be able to adopt multiple layers of security protection to prioritize the entities which are at high risk of being attacked and to minimize the damages caused by incidents.

Different from existing focuses on detection, the scope of this new regulation should be mainly emphasizes on cybersecurity incident prediction, because, when a cybersecurity threat is detected, there is a high possibility that severe damages have already been caused, such as data leakage, financial losses, and even reputation damages. On another hand, a proactively predicting approach of cyber incidents based on observed field of cybersecurity threats can fill the gap, which motivates regulators to perform a review of the former regulation.

In conclusion, when trying to predict cybersecurity incidents, it should be understood that data analytics and collection play the crucial role in the process of analysing cyber threats, modelling prediction problems and discovering security incidents, which leads that this role cannot be upon national authorities but requires an overall view that only international body as ENISA is able to provide.

Table 3: eIDAS Regulation

Rules and principles	eIDAS	Technical and organisational measures
Risk assessment and security measures	Article 19	**Technical measures** Authentication factors, which can be divided into the following categories: • Knowledge-based factors (for example: PINs, passwords, memorable words or dates, pass phrases, pre-registered knowledge and other information likely to only be known by the subject);

		• Possession-based factors (for example: asymmetric cryptographic (private) keys, the private keys may be stored on dedicated hardware devices (e.g. smartcards), or software token, uniquely identifiable token (e.g. the SIM card of a cell phone) or devices with one-time-passwords (e.g. "RSA-Token" or printed cards); • Inherent factors (variance even between people of similar characteristics so that a person may be uniquely identified, for example: fingerprints, palm prints, palm veins, face, hand geometry, iris, etc.).
Data protection by design and by default [68]	Article 12.3.c	**Technical measures** • Software development methodologies have inspired the approach to use a catalogue of specific design patterns to develop solutions to known security problems • Risk management framework and engineering objectives identify a privacy risk model and three privacy system objectives on top of the classical security objectives represented always by confidentiality, integrity and availability: predictability, manageability and disassociability (US NIST)
Notifications, reporting obligations, and	Recitals 31, 38, 39 Article 19.2	**Organisational measures** Notification can be directed to the user or be done by publishing the required information on the website of the

[68] Source: Opinion 5/2018 Preliminary Opinion on privacy by design – European Data Protection Supervisor

mitigation measures		provider depending on its content of the change and national law, which means that an application or a software to provide a document or to fill a form could be useful in case of incidents.
Business Continuity, Disaster Recovery, and Resilience	Article 10.3 Article 24.2.h and 24.2.i	**Organisational measures** It begins with a business impact analysis and a threat analysis that identifies events that could cause an interruption of business operations and processes. Following the threat identification, a risk assessment must be performed to determine the impact of the threat on the business, likelihood of occurrence, and recovery time necessary for essential business applications and processes. These activities must be performed with the full involvement of the owners of the business data and business processes, accordingly to new technologies such as: risk management, vulnerability management, identification and prioritization of business processes and supporting applications, etc.
Certification process	Recitals 44 Recital 55	**Organisational measures** Assessment of Standards related to eIDAS[69]: in this report, ENISA presents aspects of qualified electronic signature creation devices (QSCD certification) and qualified trust services provider (QTSP supervision) to identify the way to combine respective elements therein, in line with the eIDAS requirements. **Technical measures** The above-mentioned repot seeks to support standards CEN EN 419 241-2 and CEN EN 419 221-5:2018 so that

[69] https://www.enisa.europa.eu/publications/assessment-of-standards-related-to-eidas

		they could be referenced in an amended version of CID (EU) 2016/650.
Annual report to the European Authority	Article 19.3 (report to ENISA)	**Organisational measures** The wide legislation with the objective to have consistency and harmonization across the EU shows the need for preventing cyber security incidents and they had started up, for example, voluntary or mandatory incident reporting schemes to create more transparency about cyber security incidents. **Technical measures** The focus is to ensure the vital infrastructure for the digital society, the electronic communication networks and services, which entails: • Application or software open source to report easily and readily • Technologies capable to classify annual incidents • Set of capabilities to create cluster for sectors and industries.

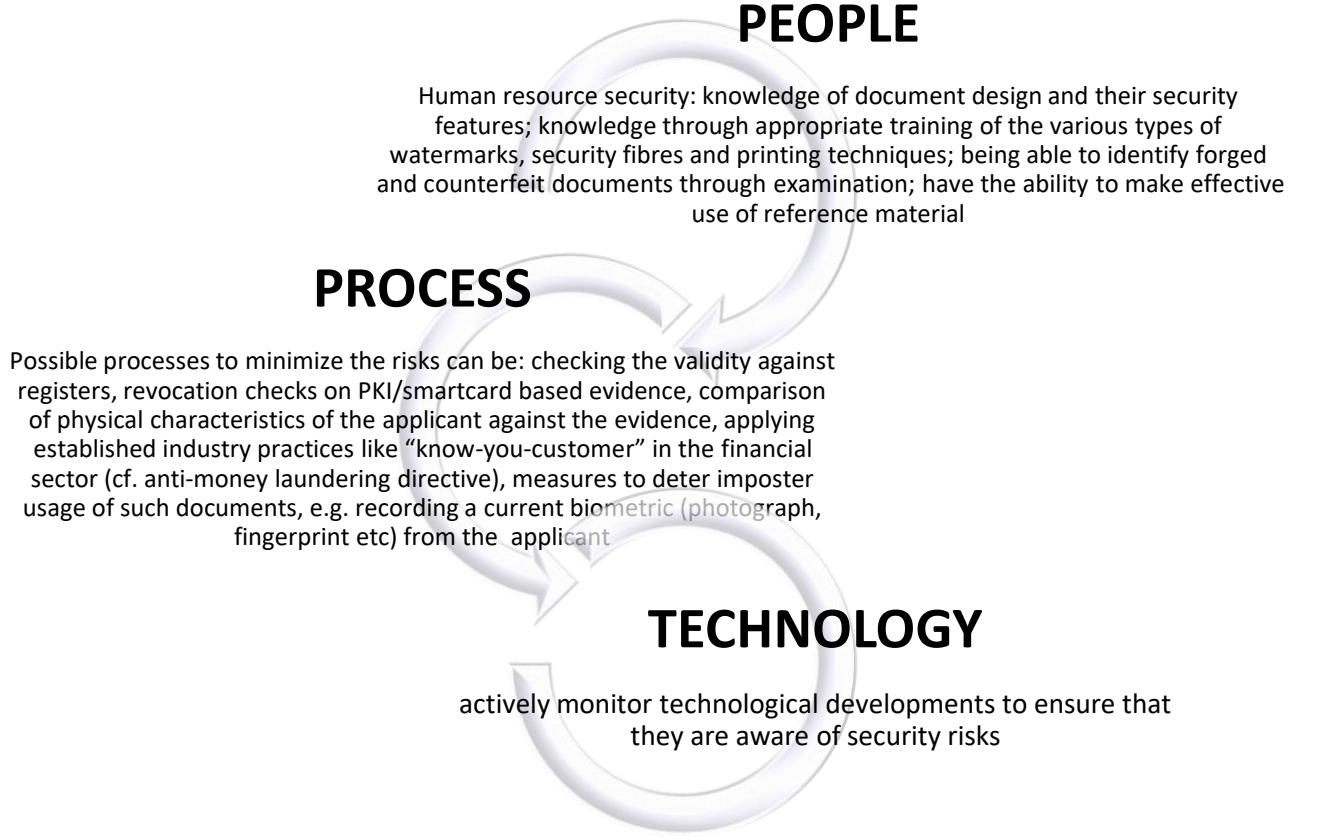

Figure 2: eIDAS Regulation

5 The NIS Directive framework

5.1 Introduction

The European Union recognized that cyber security incidents could affect a large number of Member States, leading in 2013 to a proposal to improve the EU's preparedness for cyber-incidents. This proposal became the NIS Directive[70] which, in August 2016, regulated on the security of Networks and Information Systems, giving Member States 21 months to implement this new regulation in the national laws.

The directive applies to the essential services sector, which includes companies and organizations identified as either operators of essential services (OES) or Competent Authorities (CAs). The NIS directive applies also to network and information systems which, accordingly to Article 4 of the Directive, are all electronic communications, any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data or digital data stored, processed, retrieved or transmitted by elements covered for the purposes of their operation, use, protection a maintanance.

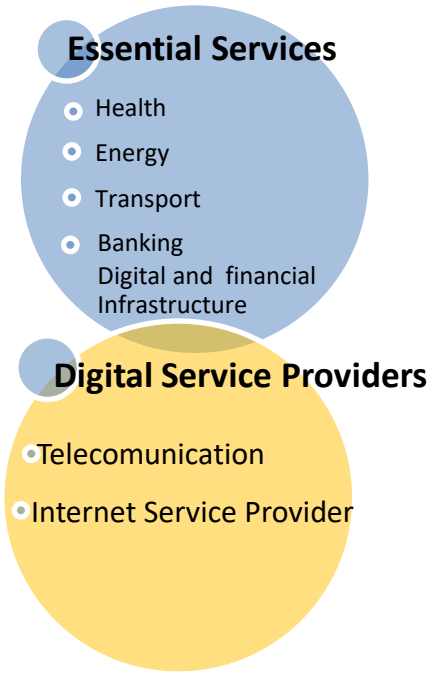

Figure 3: NIS Directive_1_Scope

[70] 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.

The NIS Directive aims to achieve the following four different goals: i) managing security risk, ii) protecting against cyber-attack, iii) detecting cyber security events, and iv) minimizing the impact of cyber security incidents.

In the following chapter, it will be taken a closer look at these objectives, discuss the current status, and how the landscape might change in the future.

5.2 Preliminary key-points of potential data protection issues

Some crucial recitals have to be analysed in order to understand properly the meaning of this regulation. Recital n. 49 provides that digital service providers should ensure a level of security proportionate to the degree of risk posed to the security of the digital services they provide, given the importance of their services to the operations of other businesses within the EU. Consequently, it has been noted that for businesses within the EU, a national risk-assessment is fundamental in order to improve the cybersecurity awareness. This assessment (1) provides capacity building activities through the production of guidelines on cybersecurity legislation, regulation and technology; (2) asserts the need and importance for countries to establish national computer incident response teams (CIRTs); (3) provides fundamental tools to develop a national cybersecurity strategy. Countries must consider the importance of National Cybersecurity Strategy as a toolkit to support the creation or enhancement of their national security. These are critical elements and frameworks for any country's socio-economic security.

Other important principles are stated in Recital n. 57 and 58 and focuses on notification requirements. Both underline that the directive must be implemented considering that applies to a cross-border contest, which means that National Legislators have to carry out an international approach when they legislate.

Member States should be able to identify the relevant operators of essential services and impose stricter requirements. In addition, this Directive and the implementing acts should ensure a high level of harmonization for digital service providers with respect to security and notification requirements. This should enable digital service providers to be treated in a uniform way across the EU, proportionally to their nature and the degree of risk.

The Directive highlights the possibility of Member States to impose security and notification requirements on entities that are not digital service providers, without prejudice to Member States' obligations under Union law.

The competent national authorities, as defined in this Directive, are required to share information securely and in compliance with the latest technologies. Accordingly, Recital n. 59 dictates that these authorities should pay due attention to preserving informal and trusted channels of information- sharing.

Publicity of incidents reported to the competent authorities should duly balance the interest of the public, in being informed about threats, against possible reputational and commercial damage for the operators of essential services and digital service providers reporting incidents. In the implementation of the notification

obligations, competent authorities and the CSIRTs should consider the need to keep information about product vulnerabilities strictly confidential, prior to the release of appropriate security fixes.

Furthermore, the Directive states the power of the Authorities to obtain sufficient information in order to assess the level of security of network and information systems (Recital 61).

NIS Cooperation Group[71]
The NIS Cooperation Group has been established by the 2016 Directive on security of network and information systems (the NIS Directive) to ensure strategic cooperation and the exchange of information among EU Member States in cybersecurity. The Group's overall mission is to achieve a high common level of security of network and information systems in the European Union. It supports and facilitates the strategic cooperation and the exchange of information among EU Member States. The NIS Cooperation Group's tasks are explicitly described in Article 11 of the NIS Directive. On the operational side, the NIS Cooperation Group is supported by the work of the network of Computer Security Incident Response Teams (the CSIRT s Network), dedicated to sharing information about risks and ongoing threats and cooperating on specific cybersecurity incidents. The CSIRT s Network was established under Article 12 of the NIS Directive which also defines its role. The NIS Cooperation Group provides strategic guidance for the activities of the CSIRT s network.

5.3 Cybersecurity obligations of NIS Directive

The NIS Directive, at Article n. 1, outlines the following main goals, with a view to achieving a high common level of security of network and information systems within the EU:

- Create obligations for all Member States to adopt a national strategy on the security of network and information systems
- Create a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them
- Create a computer security incident response team network (‘CSIRTs network’) in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation
- Establish security and notification requirements for operators of essential services and for digital service providers

[71] Source: https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

- Lay down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems.

In this regard, Article 4 provides some fundamental definitions within the framework of this Directive. The first crucial notion is the definition of risk, which is considered as "any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems".

Further important definitions concern the notion of *security of network and information systems*, which highlights the ability of network and information systems to resist, at a given level of confidence, against 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.

Finally, from an organizational perspective, the Directive adopts the notion of *national strategy on the security of network and information systems* as a framework providing strategic objectives and priorities on the security of network and information systems at national level.

Moreover, Article n. 7 provides the meaningful points for this National strategy which has to be defined by each Member State. Particularly, the national strategy on the security of network and information systems shall address the following issues:

- The objectives and priorities of the national strategy on the security of network and information systems
- A governance framework to achieve the objectives and priorities of the national strategy on the security of network and information systems, including roles and responsibilities of the government bodies and the other relevant actors
- The identification of measures relating to preparedness, response and recovery, including cooperation between the public and private sectors
- An indication of the education, awareness-raising and training programs relating to the national strategy on the security of network and information systems
- An indication of the research and development plans relating to the national strategy on the security of network and information systems
- A risk assessment plan to identify risks
- A list of the various actors involved in the implementation of the national strategy on the security of network and information systems.

To perform this activities, Member States may request the assistance of ENISA in developing national strategies on the security of network and information systems.

National Cybersecurity Strategy
The National Cyber Security Strategy sets out the government's plan to make every European country secure and resilient in cyberspace.

For instance, on September 2019, In Italy a decree on information security has been enacted. The national cybernetic security systems must be aimed at guaranteeing, in particular, the maximum level of security of networks, information systems and information services of public administrations. Specifically, the objective is the creation of the "perimeter of national cyber security". Accordingly, Italian law provides for the drawing up of a list of subjects, "national, public and private operators, on whom the exercise of an essential function of the State depends, or the provision of a service essential for the maintenance of civil, social or economic activities fundamental to the interests of the State and whose malfunction, interruption, even partial, or improper use, may result in prejudice to national security".

It is important to note that this definition could extend the scope of application of the tasks to entities other than those indicated in the NIS.

The following is the state of art of European Countries:

Table 4: National security strategies – EU Member States

Bulgaria	National Cyber Security Strategy "Cyber Sustainable Bulgaria 2020 13/07/2019
Croatia	The National Cyber Security Strategy of Republic of Croatia 07/10/2015
Cyprus	not published yet
Czech Republic	The National Cyber Security Strategy of Czech Republic for 2015 to 2020
Denmark	Danish Cyber and Information Security Strategy - 05/2018
Estonia	Cyber Security Strategy: 2014 – 2017
Finland	Information Security Strategy for Finland - 09/2016
France	Strategie Nationale Pour la Security du numerique
Greece	Greek Cybersecurity National Strategy - 03/2018
Hungary	not published yet
Ireland	National Cyber Security Strategy 2015 2017
Italy	National Plan for Data Protection and Cybersecurity - 03/2017
Latvia	Cybersecurity of Strategy of Latvia: 2014 to 2018 - 03/2017
Lithuania	National Cybersecurity Strategy - 08/2018
Luxembourg	National Cybersecurity Strategy III - 26/01/2018
Malta	not published yet
Netherlands:	Dutch Cybersecurity Agenda - 21/04/2018

Poland	Polish National Cybersecurity Strategy - 30/11/2017
Portugal	Portuguese National Cyber Security Strategy - 28/05/2015
Romania	not published yet
Slovakia	Cybersecurity Act of The Slovak Republic for 2015-2020
Slovenia	Cyber Security Strategy: Establishing a System to ensure High Level of Cyber Security - 02/2016
Spain	National Cybersecurity Strategy – 2013
Sweden	National Cybersecurity Strategy 22/06/2016
UK	National Cyber Security Strategy 2016 to 2021 - 11/2016

CSIRT – Computer Security incident Response Team[72]

The objective of the Directive is to achieve a high common level of security of network and information systems within the EU, by means of improved cybersecurity capabilities at national level, increased EU-level cooperation and risk management, incident reporting obligations for operators of essential services and digital service providers.

To achieve this goal, the NIS Directive (Article 12) establishes the CSIRTs Network "to contribute to developing confidence and trust bet ween the Member States and to promote swift and effective operational cooperation". The CSIRTs Network is a network composed of EU Member States' appointed CSIRTs (Computer Security Incident Response Teams) and CERT-EU (CSIRTs Network members). The European Commission participates in the network as an observer. ENISA is tasked to actively support the CSIRTs cooperation, provide the secretariat and active support for incident coordination upon request.

The CSIRTs Network provides a platform where members can cooperate, exchange information and build trust. Members will be able to improve the handling of cross-border incidents and even discuss how to respond in a coordinated manner to specific incidents.

The Computer security incident response teams (CSIRTs), see Article n. 9, has to be designated by each Member State in order to comply with the requirements set out in point (1) of Annex I of the NIS Directive, covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well-defined process. A CSIRT may be established within a competent authority.

[72] Source: https://www.enisa.europa.eu/topics/csirt-in-europe/csirt-network

Member States shall ensure that the CSIRTs have adequate resources to effectively carry out their tasks and access to an appropriate, secure, and resilient communication and information infrastructure at national level. Moreover, Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network and they may request the assistance of ENISA in developing national CSIRTs

The Chapter III is focused on **cooperation** and Articles n. 11 and 12 define respectively the Cooperation Group and the CSIRTs network.

In order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence (and with a view to achieving a high common level of security of network and information systems in the EU) a Cooperation Group is established. Furthermore, in order to contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation, a network of the national CSIRTs is established.

The Directive also underlines the important of the International cooperation (Article 13), providing that the EU may conclude international agreements, with third countries or international organizations, allowing and organizing their participation in some activities of the Cooperation Group. Such agreements shall take into account the need to ensure adequate protection of data.

The fourth Chapter of the Directive concerns the Security of the Network and information Systems of operators of essential services.

Article 14 provides the **security requirements** and **incident notification** and appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems. It also required that Member States shall ensure that operators of essential services take appropriate measures to prevent and minimize the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.

This leads to the necessity for providers and operators to implement business continuity and disaster recovery plans.

Furthermore, Member States have to ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.

The criteria in order to determine the significance of the impact are three:

- The number of users affected by the disruption of the essential service
- The duration of the incident
- The geographical spread with regard to the area affected by the incident.

The fifth Chapter is focused on Security of the Network and information Systems of Digital Service Providers. The provision at Article n. 16 is slightly different from Article n. 14 in order to achieve different parameters of the cyber security according to this specific sector.

Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services.

Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements:

- The security of systems and facilities
- Incident handling
- Business continuity management
- Monitoring, auditing and testing
- Compliance with international standards.

Regarding **notification**, Member States shall ensure that digital service providers notify the competent authority or CSIRT without undue delay of any incident having a substantial impact on the provision of a service that they offer within the Union. Notifications shall include information to enable the competent authority or CSIRT to determine the significance of any cross-border impact. Notification shall not make the notifying party subject to increased liability.

To determine whether the impact of an incident is substantial, the following parameters in particular shall be taken into account:

- The number of users affected by the incident, in particular users relying on the service for the provision of their own services
- The duration of the incident
- The geographical spread with regard to the area affected by the incident
- The extent of the disruption of the functioning of the service
- The extent of the impact on economic and societal activities.

The obligation to notify an incident shall if the digital service provider has access to the information needed to assess the impact of an incident against the parameters referred to in the first subparagraph.

Articles 14 to 16 of the Directive state that companies must implement appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which they use in their operations. Those measures – which should be up to speed with the current state of the art – shall ensures shall ensure a level of security of network and information systems appropriate to the threat.

Furthermore, these articles provide the obligation to notify data breaches to the Computer Security Incident Response Team (CSIRT), the Data Protection Authority and individuals when such breaches affect the rights and freedoms of personal data subjects involved in a breach.

In conclusion both operators of essential services and digital service providers are required to implement a similar level of security, adopting specific parameters in order to prevent breaches of security and loss of integrity, which lead to the obligation to notify these kinds of incidents.

Costs of Cybercrimes[73]

Cybercrime now costs the world almost $600 billion, or 0.8 percent of global GDP, according to a new report by the Center for Strategic and International Studies (CSIS) and McAfee. Scheduled for release February 21, "The Economic Impact of Cybercrime: No Slowing Down" updates the popular 2014 report, which put global losses at close to $500 billion, or 0.7% of global income.

Nearly two-thirds of people who use online services (more than two billion individuals)—have had their personal data stolen or compromised and the phenomenon is world-wide.

Actually, cybercrimes concern North America, Europe and Central Asia, East Asia & the Pacific, South Asia, Latin America and the Caribbean, Sub-Saharan Africa and MENA. Cost of cybercrime across regions depends on each country level of cybersecurity maturity, which is measured according to these key indicators: legal measures, technical measures, organizational measures, capacity building, and cooperation. As you might expect, wealthier nation-states suffer higher cybercrime losses.

- Brazil: it is the second leading source of cyberattacks and the third most-affected target.
- Germany: this country has the most sophisticated underground internet economy in the EU
- Japan: previously protected from cybercrime because of the language barrier and no infrastructure for money laundering, Japan is seeing an increase, especially in attacks targeting banks.
- United Kingdom: online fraud and cybercrime account for nearly half of all crimes, amounting to more than 5.5 million offenses annually
- United Arab Emirates: it is the second most targeted country in the world, with the cost of cybercrime estimated at $1.4 billion per year.

5.4 Summary of security obligations

Analyzing the safeguarding and information obligations imposed by the NIS Directive on operators of essential services and digital service providers, it has to be considered that to comply with these requirements, companies and organizations are required to engage in a best-efforts security risk management process aimed at identifying, assessing, and addressing risks, in order to reduce the risk of service disruptions that could lead to damages for economic and social activities.

By inspecting and analyzing the whole legislative framework, the importance of notifications and international coordination, in order to tackle the risk of cybercrimes appears paramount.

First, this regulation requires security measures strictly linked to the level of risk, which is a requirement consistent with the entire legislative European framework in this field.

[73] https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf

Second, the NIS Directive clarifies that self-reporting incidents externally detected by a third party can lead to develop higher levels of cross-border protection of Network and Information Systems. This leads to important obligations of notification and reporting.

Finally, the NIS Directive sets ups different institutional roles for cybersecurity, amongst which we note the Cooperation Group for strategic cooperation and exchange of information between Member States, as well as a network of computer security incident response teams ('CSIRTs') and ENISA.

Table 5: NIS Directive

Rules and principles	NIS Directive	Technical and organisational measures
Risk assessment and security measures	Recital 49 Article 14.1, 14.2 and Article 16.1 and 16.2	**Technical measures** According to Verizon's 2018 Data Breach Investigation Report, 96% of the attacks started with email, so records for DKIM (Domain Keys Identified Mail), SPF (Sender Policy Framework) and DMARC (Domain-based Message Authentication, Reporting and Conformance) are basic measures able to protect data. This software has to be developed and applied to other fields such as: • Software management • Access control • Authentication factors
Data protection (security) by design and by default	N/A	
Notifications, reporting obligations, and mitigation measures	Article 9. 4 Article 14.3 and 14.4 Article 16.3 and 16.4	**Organisational measures** Providers and operators must immediately report significant disruptions to the National Agency and reporting obligations must not have a negative effect on correcting the disruption. **Technical measures**

		Technologies supporting notification and reporting obligations have to: • Adopt alerting systems • Collect information on incidents • Provide specifications on what defines a significant disruption according to the law • Provide information on security issues • Provide automatizations in order to fill the notification readily according to parameters of NIS (number of users affected, duration of incident, geographic spread, the extent of disruption of the service, the impact of economic and social activities)
Business Continuity, Disaster Recovery, and Resilience	Recitals 69 Article 14.2 and Article 16.1.c	**Organisational measures** Operators and providers must ensure cyber-resilience, which mean implementing business continuity management measures such as: • Cyber risk and vulnerability management • Incident response team • Alternative resources to use in case of crisis • Back- up systems
Certification process	N/A	
Annual report to the European Authority	Article 11.3.j (Commission provides examining, on an annual basis, the summary reports referred to in the second subparagraph of Article 10 (3) (notifications))	**Organisational measures** It is important for operators and Providers to get actively involved and supported by the European Commission, ENISA, the cyber security national competent authorities and industry sector

		actors in their efforts and actions in the context of the NIS Directive rollout. The report is an element of this framework. **Technical measures** • Resource to assist in successfully handling information necessary for the report • Channels with strong authentication to collect and store data about incidents required to fill the report • Structural support to target and seclude data and information about incidents • Secure channel to share information with the Commission

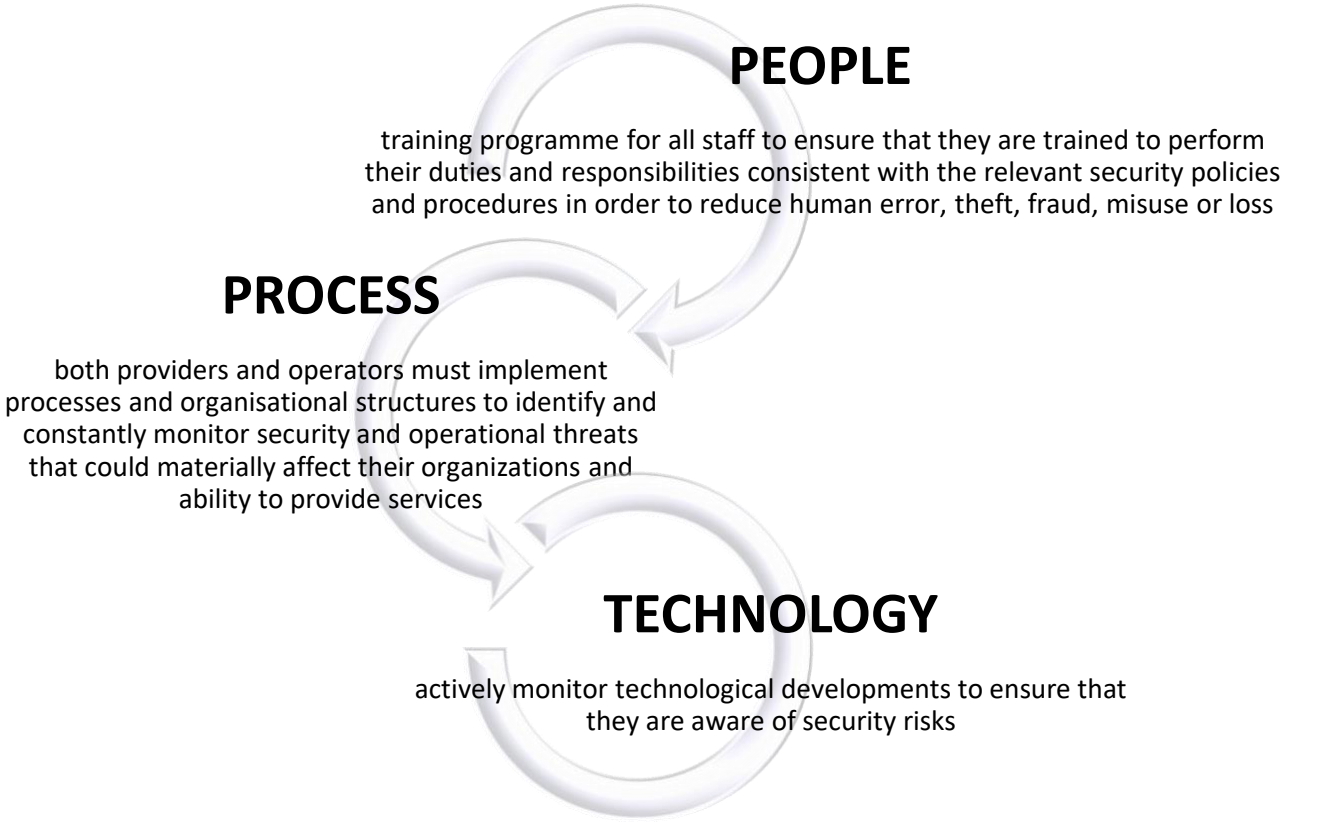

Figure 4: NIS Directive_2

6 The draft of the proposed e-Privacy Regulation

6.1 Introduction

The adoption of the Regulation 2016/679/EU, the General Data Protection Regulation[74](GDPR) was a key element for the reform of the personal data protection legal framework. The adoption of GDPR fulfilled the objectives of Digital Single Market Strategy (DSM Strategy) to increase trust and security of digital services but this was not enough. DSM Strategy likewise noticed the necessity of reviewing the existing legal framework in electronic communications services. Directive 2002/58/EC[75] (e-Privacy Directive), which was amended by the Directive 2009/136/EC[76], should have been reviewed in order to provide a high level of privacy protection for users of electronic communications services and reinforce trust and security in the Digital Single Market[77]. For this reason, European Commission in January 2017 proposed the e-Privacy Regulation, a Regulation on Privacy and Electronic Communications.

The future e-Privacy Regulation[78] intends to replace the existing e-Privacy Directive and aims to implement article 7[79] of the Charter of Fundamental Rights of the European Union (Charter) that protects the fundamental right to the respect for private life with regard to communications. E-Privacy Regulation comes to provide additional strong guarantees for all types of electronic communications and support GDPR. GDPR implements article 8[80] of Charter which provides protection of personal data. This is the reason why

[74] 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).
[75] 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).
[76] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.
Article 2 of Directive 2009/136/EC amended the e-Privacy Directive and at first introduced the obligation of the telecommunication providers to report any data breach to regulatory authorities and to the affected individuals. The obligation of reporting was the result of Article 4(1) of the e-Privacy Directive, which states that *"providers of electronic communications service must take appropriate technical and organizational measures to safeguard security of its service…"*.
[77] https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.
[78] Draft Regulation of the European Parliament and of the Council concerning the respect for privacy life and the protection of personal data in electronic communications and repealing Directive 2202/58/EC (Regulation on Privacy and Electronic Communications).
[79] Article 7 - Respect for private and family: "Everyone has the right to respect for his or her private and family life, home and communications."
[80] Article 8 – Protection of personal data: "1. Everyone has the right to the protection of personal data concerning him or her.

lawmakers proposed the e-Privacy, to complete and to particularize GDPR[81]by laying down specific rules for the purposes mentioned in paragraphs 1 to 2 of article 1 of the ePrivacy Regulation Again, the form of Regulation as a regulatory instrument was preferred to ensure common legal provisions for all member states, to avoid divergences among countries and to ensure consistency with the GDPR. Moreover, the Regulation is directly applicable to all member states without waiting each country to transfer the new legal rules to its national legislation. The European legislator, in 2013, had passed the Regulation 611/2013 which tried to complement the existing rules and to harmonize data breach notification requirements by public electronic communications service providers[82].

E-Privacy Regulation applies to electronic communications. By using the term "electronic communications" we mean "transmission systems, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed" as it is defined in article 2 (1) of Directive establishing the European Electronic Communications Code.[83] In other words, it covers any content that is exchanged and transferred by electronic means, including text, images, videos, speech and metadata. Article 5 of the draft proposal of e-Privacy regulation highlights confidentiality of electronic communications data and states that "any interference with electronic communications data, such as by listening, tapping, storing, monitoring, scanning or other kinds of interceptions, surveillance and processing of electronic communications data, by anyone other than the end-users concerned, shall be prohibited"[84]. Article 6 at the same time performs a list of cases that processing of electronic communications data is permitted. E-Privacy covers all cases of communications such email, apps, telephone, instant messaging etc.

The study that follows, is based on the latest version/draft of the proposal of ePrivacy Regulation which was published in November 2019. Since, there are still debates and negotiations on several parts of this proposal, member states have not yet agreed to the final version of the future ePrivacy Regulation. As a result, updated

---

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."

[81] Article 1 (3) of the draft proposal of e-Privacy.

[82] Regulation (EU) 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications.

[83] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast).

[84] Examples of interception of electronic communications data, given in recital 15 of the draft of the ePrivacy Regulation, are when someone external person listens, reads, scans or stores the content of electronic communications or the associated metadata for other purposes than the parties of the communication wish. Other examples are the monitoring from third parties of websites visited, timing of the visits, interaction with others, capturing payload data or content data from unecrypted wireless networks and routers, including browsing habits, etc.

versions[85] of the ePrivacy Regulation have been published from the first draft that was published in January 2017. Bulgarian, Austrian and Romanian and Finnish Council presidencies have attempted to facilitate and complete the procedures for the final version of the ePrivacy Regulation by publishing new drafts of the legal document. However, the efforts failed and there are still disagreements between the member states. At the next step, Croatian presidency (after January 2020) has the turn to propose a new draft of the ePrivacy Regulation. Bearing in mind the delays of this new regulation, it seems that it will not enter into force before 2023 (into effect before 2025).

6.2 Consequences of the future e-Privacy Regulation in cybersecurity

With no doubt, e-Privacy Regulation comes to enforce a common legal framework in telecommunications for all the EU member states. It is going to replace the e-Privacy Directive, known as "cookie law". However, the new Regulation is going to address more issues and not being focused only on "cookies". The most important topics that this future Regulation will address are the following:

6.2.1 Protection of legal entities

Confidentially of electronic telecommunications is very crucial not only for natural persons but also for legal entities. Lots of electronic communications data of legal entities may reveal confidential information such as business secrets or other sensitive information that have financial value. For this reason, law makers decided to pay special attention to the protection of legal entities too. In the very beginning of the e-Privacy Regulation, in article 1a, is mentioned, that "this Regulation lays down rules regarding the protection of

[85] Updated version of 8th of September of 2017 of the future ePrivacy Regulation can be found at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_11995_2017_INIT&from=EN
Updated version of 22th of March of 2018 of the future ePrivacy Regulation can be found at https://www.bvdw.org/fileadmin/bvdw/upload/dokumente/recht/e_privacy_verordnung/Bulg.RatsP_zu_ePrivacyVO_v._22.03.2018.pdf
Updated version of 19th of October of 2018 of the future ePrivacy Regulation can be found at http://data.consilium.europa.eu/doc/document/ST-13256-2018-INIT/en/pdf
Updated version of 12th of July of 2019 of the future ePrivacy Regulation can be found at https://data.consilium.europa.eu/doc/document/ST-11001-2019-INIT/en/pdf
Updated version of 26th of July of 2019 of the future ePrivacy Regulation can be found at http://data.consilium.europa.eu/doc/document/ST-11291-2019-INIT/EN/pdf
Updated version of 18th of September of 2019 of the future ePrivacy Regulation can be found at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil:ST_12293_2019_INIT
Updated version of 4th of October of 2019 of the future ePrivacy Regulation can be found at https://data.consilium.europa.eu/doc/document/ST-12633-2019-INIT/EN/pdf
Updated verion of 8th of November of 2019 of the future ePrivacy Regulaton can be found at https://data.consilium.europa.eu/doc/document/ST-13808-2019-INIT/en/pdf

fundamental rights and freedoms of legal persons in the provision and use of electronic communications services and in particular their rights to respect of communications".

At this point, it is important to mention that the scope of article 7 of the Charter and article 8 of the ECHR also apply to the protection of professional activities of legal entities according to the case-law of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECHR)[86]. As a result, legal entities are treated as "end-users" and whenever protection of "end-user" is mentioned in the e-Privacy Regulation, it also refers to legal entities. According to recital 3 of the draft proposal of e-Privacy, the provision of GDPR should also apply to legal entities, which means that the legal entities should have similar rights as end-users as natural persons. This becomes very clear in article 15 (3) which states that the providers of number-based interpersonal communications services shall provide end-users that are legal persons with the possibility to object to data related to them being included in the directory. Article 15 (3a) continues by stating that the providers of number-based interpersonal communications services shall give end-users the means to verify, correct and delete such data included in a publicly available directory

Additional protection to the legal entities from unsolicited communications is given under Article 16 (5) of the proposal of e-Privacy Regulation. The broaden protection of professional activities and communications will with no doubt positively influence internal market and increase trust for marketing purposes.

6.2.2 Regulation of content and associated metadata

Through the electronic communication systems, lots of information may be shared. This content, which includes personal data, sometimes may be characterized as sensitive since it usually reveals personal preferences, political views, medical conditions, sexual preferences, emotions, habits, etc. Not only the personal data, but also the metadata may be deduced by electronic communications and may reveal sensitive and personal information. By using the word "metadata", we mean the data that provides information about other data[87]. Article 4 (3) (a) of the e-Privacy Regulation mentions that "electronic communications metadata" is included in the general term of "electronic communications data". Moreover, recital 14

[86] Explanatory memorandum of the e-Privacy Regulation, 2.1. See also Case C-450/2006, Varec SA v Etat belge, paragraph 48 states "the notion of 'private life' cannot be taken to mean that the professional or commercial activities of either natural or legal persons are excluded". Case of Niemietz v Germany, paragraph 29 states "There appears to be no reason of principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world. This view is supported by the fact that, as was rightly pointed out by the Commission, it is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not. Case of Colas Est and Others v France, paragraph 41 states "the Court considers that the time has come to hold that in certain circumstances the rights guaranteed by Article 8 of the Convention may be construed as including the right to respect for a company's registered office, branches or other business premises". Case of Peck v The United Kingdom, paragraph 57 states "Private life is a broad term not susceptible to exhaustive definition. The Court has already held that elements such as gender identification, name, sexual orientation and sexual life are important elements of the personal sphere protected by Article 8. That Article also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world and it may include activities of a professional or business nature."

[87] https://en.wikipedia.org/wiki/Metadata.

highlights that electronic communications data should be defined broadly in a technology neutral way so as to cover any information related to the content transmitted or exchanged. Metadata includes information like numbers called, the websites visited, geographical location[88], the time, date and duration of a specific call. All those information that can by derived from the electronic communications may disclose important information for the personal and private life of an end-user. Moreover, in case of the correlation of all those data, information from social activities, interests, habits and everyday life can be revealed[89]. Court of Justice of the European Union also recognized that metadata may reveal very personal and sensitive information[90]. According to article 6a (1) (b) such (meta)data can be processed only if all end-users concerned have given their consent to this processing for one or more specified purposes.. Prior, the provider has to carry out an assessment of the impact of the processing and consult the supervisory authority. For the consultation of the supervisory authority, article 36 (2) and (3) of GDPR is applied. Additionally, the possibility of a data protection impact assessment has to be examined in cases of high risks to the rights and freedoms of natural persons[91].

6.2.3 Changes on "cookies"

The e-Privacy Directive 2002/58/EC which is going to be replaced by the e-Privacy Regulation, is likewise known as "The cookie Directive"[92]. The provisions of the "cookie Directive" obliged the website owners to receive visitor's consent in order to retrieve any tracking information on a computer or mobile device. The aim of these legal changes was to make internet users be aware of how their information is collected and processed by the website owners and give them the opportunity to accept or refuse this type of processing. As a result, internet users, constantly, by visiting several websites, are asked to provide their consent in

[88] However, in recital 17 it is stated that "location data that is generated other than in the context of providing electronic communications services should not be considered as metadata".
[89] Recital 2 of the proposal of e-Privacy Regulation.
[90] C-293/12 and C-594/12, para. 26 and 27 state "… date, time, duration and type of a communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services. Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period. Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."
[91] Recital 17 of the proposal of ePrivacy Regulation.
[92] Cookies definition: "A cookie is a small piece of data that a website asks your browser to store on your computer or mobile device. The cookie allows the website to "remember" your actions or preferences over time", http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm.

order to have full access to those websites. However, the current situation seems to be annoying for the internet users who are overloaded with requests to provide their consent[93].

EU legislator, in recital 20 (a) of e-Privacy Regulation, points out that implementation of technical means in electronic communications software to provide specific and informed consent through transparent and user-friendly settings, can be useful to address this problem issue.

More specifically, it is proposed that advanced technical means can be used for the consent in order to address the problem in a friendly for the user and transparent way. Moreover, providers of software are encouraged to include settings in their software which allows end-users, in a user friendly and transparent manner, to manage consent to the storage and access to stored data in their terminal equipment by easily setting up and amending whitelists and withdrawing consent at any moment.[94]

e-Privacy Regulation also wants to address the cookies fatigue by providing an exception to the obligation of obtaining consent is some cases of no involvement or only very limited intrusion of privacy happens to the end-user. Pursuant to Recital 21, the storage of cookies for the duration of a single established session on a website, does not need any prior consent from the end-users since this is a strictly necessary thing for having full access to the website. It is likewise absolutely legitimate to collect cookies for website statistic purposes without being obligatory to have a consent.

6.2.4 New applications and providers

One more issue that the e-Privacy Regulation tries to address is to include more electronic communication services in to its scope. The current legal framework, since the last version of the ePrivacy Directive in 2009 does not seem to follow the technological development living a gap of protection of communications expressed through new services. On the other hand, end-users (consumers and businesses), prefer more and more inter-personal communications like Voice over IP, instant messaging, email and leave behind traditional communications services[95]. Therefore, the future ePrivacy Regulation applies to any organization that provides any form of online communication service, such as the website owners, messaging service providers (eg. Skype, Facebook, etc.), owner of apps that provide electronic communications, telecommunications companies, internet service providers, etc.

Through Recital 12 of the draft ePrivacy proposal, moreover, we easily realize that the EU legislator focuses on the communication of connected devices and machines by using electronic communications networks (internet of Things). This communication and transmission between different devices and machines, may constitute electronic communication services. Consequently, confidentiality and security, if we want to talk

[93] It seems that the current situation with cookies consent is both over-inclusive and under-inclusive. Over-inclusive since it usually covers non-privacy related issues and under-inclusive because it usually does not clearly cover some tracking techniques used by the provider.
[94] Recital 20 (a) of the proposal of e-Privacy Regulation.
[95] Explanatory memorandum of the e-Privacy Proposal, 1.1.

about secured and trusty communications, should also cover the communication of connected devices and/or machines.

6.2.5 Unsolicited marketing

e-Privacy Regulation likewise aims to regulate spam issues, issues related to unsolicited marketing. More specifically, article 16 of the Regulation tries to provide more safeguards to the end-users in order to protect them from unsolicited and direct marketing communications. Independently from the means of marketing communications (automated calling and communications system, messaging applications, emails, SMS, MMS, Bluetooth, telephone, etc.)[96], the natural or legal persons who wish to use electronic communications service for the purposes of sending direct marketing communications should have the prior consent from the end-users [Article 16 (1)]. Of course, there are cases of already existing mailing and emailing lists that before the time the e-Privacy will come into force. In such situations, the use of those communications lists of customers is legitimate since it happens within the context of an existing relationship, which offers similar products and services[97]. In any case, the consent should be given according to the details of GDPR, and in order for the data subject to be able to communicate the data controller and possibly to exercise his/her rights, the contact details (usually email and telephone number) of the data controller should be available at any time. Particularly, for unsolicited direct marketing communications, lawmakers, in Article 16 (6) (a), highlighted the prohibition of identity masking or the use of false identities, return addresses or phone numbers.

6.2.6 End-user's consent

Similar to the GDPR, the proposal of ePrivacy Regulation, pays special attention to the end-user's (natural or legal person) consent[98] for processing any personal data and metadata in telecommunications. What is more, in cases of marketing purposes, valid consent of the end user is the legal basis of any kind of processing. In order for the consent to be valid, should meet all the criteria given by the definition given in GDPR (Art. 4 no. 11).

The main scope of the forthcoming ePrivacy Regulation is to keep the electronic communications confidential, which means that any interference in the telecommunications is prohibited unless the end user has provided his/her consent[99]. The only exception is the "cookies" as it is already mentioned above, where only very limited intrusion of privacy occurs.

[96] Recital 33 of the proposal of e-Privacy Regulation.
[97] Recital 33 of the proposal of e-Privacy Regulation.
[98] Definition of "consent" under Regulation (EU) 2016/679 (GDPR): "consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".
[99] Recital 15 of the proposal of e-Privacy Regulation.

An important issue related to the consent is that the end-users should be informed for the processing activities in a, as user-friendly as possible, way[100]. This will be very helpful for the end-users to actually understand the processing activities and, therefore, the consent to meet all the legal criteria in order to be valid. The consent should be given with an affirmative action by the end-user and should before any kind of processing of their data. End-users should be able at any time to withdraw their consent in an easy way, similar to the way the consent was initially given (Article 16 (6) (d) of draft ePrivacy Regulation). End-users is necessary to have clear and true contact details in order to withdraw their consent at any time without any cost[101]. . With regard to internet or voice communication, the end-user should have the free choice and be able to refuse or withdraw his/her consent without detriment, otherwise the consent is not valid[102].

For number-based interpersonal communications services, according to article 15, end-users who are natural personals who wish to be included in a public directory, should be asked for consent before the inclusion of their personal data in the directory. The personal information provided should be the absolutely necessary and the data subject should be able to choose the categories of personal data that wishes to be included in this directory (name, email address, phone number, home address, etc.).[103]

6.3 Security measures of e-Privacy

e-Privacy Regulation, for adequate and effective protection of end-users, payed major attention to security measures. When we talk about safe telecommunications, at first we mean all those technical and security measures that ensure secure and trusted telecommunications. Article 8 of draft ePrivacy Regulation, for *Protection of end-users' terminal equipment information*, in para. 2b stipulates that "… The collection of such information shall be conditional on the application of appropriate technical and organizational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of GDPR". In other words, the telecommunication providers, even in case that process of information is permitted, they have the obligation to take appropriate technical and organizational measures for the protection of end-users. At this point, we can clearly see again, the interaction of draft ePrivacy Regulation and the GDPR. The EU legislator refers to the technical measures as they are described in article 32 of GDPR[104] where an indicative list of measures is performed.

[100] Recital 20a of the proposal of e-Privacy Regulation.
[101] Recital 34 of the proposal of e-Privacy Regulation.
[102] Recital 18 of the proposal of e-Privacy Regulation.
[103] Recital 30 of the proposal of e-Privacy Regulation.
[104] Article 32 of GDPR states "… the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: a) the pseudonymisation and encryption of personal data; b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing".

Electronic telecommunication providers have likewise the obligation to inform the end-users with all the measures that they have taken for the protection of their communications. The provider is obliged to apply security measuresaccording to article 32 of GDPR[105].

EU legislator likewise pays attention to the anonymity of data and metadata of end-users. Anonymization is technique applied by the providers, which guarantees extra protection for the end-users. Article 7 of the draft ePrivacy Regulation, in paragraphs 1 and 2, refers to the provider of electronic communication services, who has the obligation to erase any electronic communication content and the metadata of it or to make it anonymous after the receipt of the content or after the end of the communication. Of course, there are exceptions to the above anonymization/erasure. The exceptions are pointed out in article 6 (1) (b) and 6a where electronic communications data is permitted.

6.4 Summary of security obligations

The key points that set obligations to the electronic communication providers for cybersecurity in the future ePrivacy Regulation, are related to the confidentiality of telecommunications and the technical and organizational measures that have to be taken in order to assure secure communication for the end users. ePrivacy does not set on tis own new methods of security and privacy, but as a complementary to GDPR legal document, refers to the latter's rules and principles. Purpose limitation and data storage limitation are mentioned to the future ePrivacy Regulation but are explained similarly to the GDPR. For the electronic communications provider, and for avoiding security risks, design by default and by design are also proposed in ePrivacy Regulation. The table below summarizes the security obligations set by ePrivacy for the electronic communication providers.

Table 6: e-Privacy

Rules and principles	e-Privacy Regulation	Technical and organisational measures
Purpose limitation	Recitals 17, 19 and 20 Article 8 (1) (a)	Similar to GDPR, e-Privacy Regulation states that "…The protection of the content of electronic communications pertains to the essence of the fundamental right to respect for private and family life, home and communications protected under Article 7 of the Charter. Any interference with the content of

[105] Recital 15aa of the proposal of e-Privacy Regulation.

		electronic communications should be allowed only under very clear defined conditions, for specific purposes and be subject to adequate safeguards against abuse...”
Data storage limitation	Article 7.1 and 7.2	The duration of processing and storage of the data has to be the strictly necessary and proportionate of the service that is used. After the completion of the communication, the content of the communication has to be erased or to **be anonymized** (by the use of the appropriate techniques) by the electronic communications service. If any data may be stored, recorded or otherwise processed, should be done **in accordance with the GDPR.** Article 8 (2b) also refers to technical and organizational measures of article **32 (2) and (3) of GDPR** that apply to ePrivacy too.
Data confidentiality	Recitals 1, 6, 11a, 12, 13, 15aa, 16, 17 and 17aa Article 5	Similar to GDPR technical and organizational measures apply here. Moreover, when processing of data is likely to result in a high risk to the rights and freedoms of natural persons a privacy impact assessment should take place according to GDPR rules prior to processing.
Detected security risks	Recital 17b Article 6b and 6c	Electronic communication providers have the obligation to inform end users for a) possible high risks that may occur while using their services and b) the measures that they have taken for the protection of the security of the

		telecommunications (encryption and pseudonymisation).

6.5 Interplay between the proposed ePrivacy Regulation and the GDPR

As it is already mentioned, the future ePrivacy Regulation and the GDPR are two different legal documents, where the former comes to complement and particularize the later (article 1(3) of the draft ePrivacy Regulation) by laying down specific rules for the purposes mentioned in paragraphs 1 and to 2 of ePrivacy Regulation.. EPrivacy Regulation refers so often to the GDPR that seems it cannot stand alone without the interaction with it. To be more precise, the future ePrivacy Regulation refers and mentions GDPR in the following cases:

- Article 4 (1) (a): many of the definitions that are used in the draft of the ePrivary Regulation are given in the GDPR;
- Article 6a (2) : providers of the electronic communications services can process electronic communications content under specific circumstances as they are described in article 6 and 6a and it is further emphasized that points (2) and (3) of article 36 of GDPR should apply in ePrivacy Regulation too;
-
- Article 8 (2a): collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment is permitted if article 13 of GDPR is fulfilled;
- Article 8 (2b): article 32 of GDPR applies too.
- Article 4a and (1) and 4 (3): definition of consent is provided in GDPR along with the possibility of withdraw of it (article 7(3) of GDPR);
- Article 11 (1): refers to the public interests as they are described in article 23 (1) (c) to (e) of GDPR in cases of restrictions;
- Article 16 (2): refers to electronic contact details of a customer obtained by another natural or legal person for direct marketing purposes under GDPR provisions;
- Article 18: the Supervisory authority/ies responsible for monitoring the application of GDPR shall be responsible for monitoring the application of the ePrivacy Regulation;
- Article 19: the European Data Protection Board established under art. 68 of GDPR shall have the responsibilities to the consistent application of Chapter I, II and III of ePrivacy Regulation too;
- Article 21 (1): refers to the remedies which are similar to GDPR
- Article 22: provisions for the right to compensation and liability of any person who have suffered material or non-material damage, as a result of an infringement of the ePrivacy Regulation, similar to article 82 of GDPR;
- Article 23 (1): conditions for imposing administrative fines, where Chapter VII of GDPR applies to ePrivacy Regulation too.

Obviously, from the abovementioned list of articles, we can come to the conclusion that when we refer to ePrivacy, at the same time we have to bear in mind GDPR as well. To better understand the relationship between the two legal instruments it would be beneficial to scope on their similarities and differences.

Both GDPR and ePrivacy are regulations that deal with privacy law, which means that they are directly applicable to member states and their subject, to a large extent, is common. Moreover, they both apply to those who process personal data of EU citizens, independently of where they, as processors, are established, within Europe or not. One more similarity is they both impose high fines to processors in case of non-compliance.

On the other side, there are many interesting differences between GDPR and the draft of the ePrivacy Regulation. Firstly, GDPR regulates issues regarding "personal data" as it is defined in Article 4 (1) and refers to any information that can identify a natural person (implements article 8 of Charter). ePrivacy Regulation aims to regulate issues related to "electronic communications" and refers to any data that can be transferred electronically independently of if it is used to identify someone or not (implements article 7 of Charter). Secondly, GDPR is applied to any type of personal data which is kept not only electronically but also in physical files, in contrast with ePrivacy which refers only to electronical files. Moreover, according to GDPR, the main responsibilities are given to the data controller and the data processor, who are the key natural or legal persons who process personal data of data subjects, but for the ePrivacy Regulation, the main responsibilities fall to the anyone that processes any kind of content of electronic communications, such as website or app owners, internet service providers, messaging or call service providers, etc. Last but not least, ePrivacy regulation aims to provide protection not only to natural persons but also to legal persons.

7 Supporting technologies and solutions

Throughout this work, different regulations were presented and each of them brought with it its own set of different requirements. The purpose of this chapter is to present some of the technologies or solutions that are necessary to fulfil the requirements, what security or privacy related feature they provide and indicate some of the crossover between the regulations (many of the requirements are achieved by the same technologies or solutions).

7.1 Privacy Enhancing Technologies (PETs)

As the name would suggest Privacy Enhancing Technologies (PETs) are a category of technologies or approaches (software or hardware) aimed at protecting the privacy of users by eliminating or reducing personal data and/or its processing, usually without losing the functionalities of the systems to which the PETs are applied. PETs are a very broad category of technologies and measures covering anything from a piece of tape masking a webcam to advanced cryptographic techniques [106]. The European Union Agency for Network and Information Security (ENISA) classified PETs into four categories [107]: Secure messaging, Virtual Private Networks, Anonymizing networks, and Anti-tracking tools for online browsing.

PETs link closely to the concept of privacy by design, which is required under the GDPR. Privacy by design demands from controllers and processors of personal data to embed privacy measures directly into the design of any systems processing personal data. However, the regulation does not specify concrete solutions to be used to achieve privacy by design. This is where PETs can come into play. By implementing different PETs, organizations can be fairly certain they are complying with data protection by design principles. However, PETs are not only useful for the protection of personal data, but also for commercially sensitive data or data related to national security. When sharing such data, it is important to only share the data that is meant to be shared and only with trustworthy persons. The difference between PETs and general cybersecurity is that the latter protects the data from being accessed, while the former is focusing on getting useful information from data, without revealing all of the data.

PETs can help achieve many things, all of which also support privacy by design paradigm and the GDPR principles of personal data protection and privacy [108]. Gaining consent, based on an informed decision from the user, for processing of their personal data has been an important principle introduced by the GDPR.

[106] The Royal Society, Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis. ISBN: 978-1-78252-390-1. Available at https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies/, last accessed 2.11.2019.
[107] ENISA PETs Controls Matrix report, 2016. Available at https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-privacy-tools, last accessed 2.11.2019.
[108] The Office of the Privacy Commissioner of Canada, Privacy Enhancing Technologies – A Review of Tools and Techniques, 2017. Available at https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711, last accessed 2.11.2019.

PETs include techniques that allow for personal data to be tagged with instructions or preferences about how this data can and should be used. The policies are machine readable and by introducing different cryptographic elements, the data can be used only by entities, that respect those preferences. This technology is still considered to be in a concept stage as it has not had much commercial success, mainly due to its complexity. Data minimization is another key GDPR privacy design principle, requiring from data controllers and processors to only process the minimum amount of data necessary for a given task. The goal is to reduce the quantity of collected personal data, so the organizations collecting the data have a smaller subsection of all of a person's personal data and in case of a data breach less data is disclosed. PETs in this category deliberately choose not to collect or store any unnecessary personal information (e.g. a search engine DuckDuckGo), or help deleting any computer activities or browsing history (e.g. Privacy Eraser), or not save browsing history (e.g. private browsing in all major modern web browsers) or ephemeral communications, where any record of conversation is automatically deleted after a set amount of time (e.g. Snapchat) or other similar solutions. PETs can be used to improve a person's abilities to track what personal data was disclosed to whom and under what conditions or to allow for transparency of online transactions. A very important issue in GDPR and for PETs to address is anonymity. Anonymity can be associated with stored data, where it should be impossible to infer about the identity of a subject from their data, and to communications, where it should be impossible to infer about the identity of the communicating parties. Probably the two best-known PETs that enable online anonymity during communication are Tor and Virtual Private Network (VPN) (when used appropriately). Another PET that has great potential are solutions that allow the user to have control over which information they share. The idea is to only share the information that is absolutely necessary (e.g. when buying alcohol, the only information the seller needs to know is that the buyer is of legal age, the remainder of personal information on the identification card is of no relevance to them). One of the more promising techniques to achieve this are attribute-based credentials. One of the more amicus concepts was the idea of personalized privacy policies, where an individual could negotiate their own policy with an online service provider. The user could specify their preferences and the web browser could tell them the practices of the site they are visiting, how they are different from their own, allow them to search for sites with certain privacy protections etc. However, as far as we can tell, this idea was not yet been successfully developed in practice.

In summary, the field of Privacy Enhancing Technologies is a very interesting and flourishing field of research. While the use of PETs is not required by any of the previously discussed legislations, their use can help achieve the required level of security and privacy. This is definitely the most obvious in the case of the GDPR, but because PETs cover such a wide array of solutions, they can be used to achieve compliance with many requirements.

7.2 Risk management

When discussing containment of risk there are three terms that are often used - Risk Management, Risk Assessment, and Risk Analysis. Each of them is slightly different from the other.

Risk management is the continual loop of identification, analysis, evaluation and finally introducing measures to reduce the organization's exposure to risk. A part of risk management is also controlling the mechanisms put into place to reduce the risk and changes to the risk itself. This makes risk management and ongoing process. After time established controls might stop working as intended, new vulnerabilities might be put into the organization processes, new threats may arise, etc., that is why it's important to continuously monitor the risks present in an organization. Risk assessment is a part of risk management. It includes processes and technologies that identify, evaluate and inform about possible risks. As it is primarily concerned with the identification and analysis of risks it is often considered the crucial part of risk mitigation process. Risk assessment can be quantitative, which means that the risks are quantified or measured in terms of definite numbers or qualitative, which is more subjective of the two and gives only a rough idea of how the organization will be affected by risks and how significant the consequences will be. Risk analysis is a part of the risk assessment. After the risks the information (or organization, or whatever else the risk we are trying to manage for) is under are identified, the analysis quantifies this risk. The result of a risk analysis is a calculation or estimation of the probability of a certain risk occurring and the loss it would cause to the organization.

Risk management starts off with the identification phase. This includes identification of assets that an organization holds. Assets can be physical, software or data. Identification also includes recognition of vulnerabilities that the organizational processes might contain and threats that could cause the assets to be compromised (e.g. natural disasters or hacking attacks). Lastly this phase also includes identification of controls. Controls are methods of addressing identified vulnerabilities and threats by remedying, mitigating or transferring them. The next phase is assessment of risks. After collecting the assets, their vulnerabilities, possible threats and what controls are already in place to protect them you can define the risks present in an organization. The formula for calculating the risks typically involve the likelihood of vulnerability being exploited or the threat manifesting itself, together with the impact this would have on the asset and the importance/value of the asset to the organization. Existing controls are included as mitigating factor. After risks have been evaluated, they are commonly ranked to give an easy overview of the most important risks. After the risks have been defined the organization must choose what to do about them. The simplest response is to do nothing and just accepting the risk. This is the best option when the risk is insignificant and fixing it would be complicated and/or expensive. The organization can choose to remedy the risk, in which case the underlying vulnerability or threat is fixed or severely reduced resulting in elimination of the risk. Another form of treatment is mitigation, where the probability and/or impact of the risk is reduced but not entirely. The risk is still possible, but less likely to occur or less damaging to the organization. Risks can also be transferred to other entities, so the organization can recover after the risks are realized (e.g. insurance). Final treatment to risk is avoidance, where the organization seeks to avoid compromising events entirely.

A Data Protection Impact Assessment (DPIA) is a legal requirement under the GDPR when the processing of data is likely to result in a high risk to the data owners. It is a process designed to help identify and minimize data protection risks. It increases the awareness of issues related to privacy and data protection within an organization. Early acknowledgement of privacy and data protection also encourages implementation of data protection by design. DPIA is, therefore, a limited form of legally required risk

management. Failure of carrying it out a when required may result in a fine of up to €10 million, or 2% global annual turnover if higher [109].

DPIA is also similar to risk management in its organization. Any DPIA must first describe the processing (on which data it is performed, when or how often, for what purpose, etc.). This is similar to asset identification in risk management. It is also required to asses the necessity of the processing of personal data, if it is proportional to the goal we are trying to achieve by processing and if such processing is compliant to the GDPR and other legislation. Based on nature and all other identified information about the processing risks for natural persons are identified and assessed. Finally, where necessary mitigation measures must be identified and enforced.

Risk management is a very important puzzle piece when ensuring privacy and security. This is also shown in the legislation, where it was mentioned in one form or another in GDPR (DPIA and separately as an independent risk management strategy), eIDAS and NIS directive.

7.3 Authentication, Authorization and Access control

Authentication, authorization and access control are similar concepts that are related to each other but still distinct. Authentication is a process of identifying someone. It serves to verify that somebody is who they claim to be. Note that the authenticated party is not necessarily a person (e.g. an application authenticating with a web application programming interface (API)). Authentication can be performed based on three different factors: Knowledge-based authentication factors, Possession-based authentication factors and Inherent authentication factors [110].

Knowledge-based authentication factor requires the subject to demonstrate knowledge of particular information. This information is presumably only known to the subject and the verifying entity, although it is possible even for the verifying entity to not know the information. In such a case the verifying entity is only able to verify that the submitted information is correct. The examples of knowledge-based authentication factor include passwords, a personal identification numbers (PINs), passphrases, pre-registered knowledge (mother's maiden name) etc. Typical attacks on knowledge-based authentication factors are guessing, phishing eavesdropping or duplication. Possession-based authentication factors require the subject to demonstrate the possession of a factor. This factor (e.g. token) is under the sole control of the owner and therefore nobody else can use it to authenticate. The security of such a method is reliant on the

[109]Information Commissioner's Office in the United Kingdom. Available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/, last accessed 3.11.2019.

[110] European Commission, Guidance for the application of the levels of assurance which support the eIDAS Regulation. Available at https://ec.europa.eu/cefdigital/wiki/download/attachments/40044784/Guidance+on+Levels+of+Assurance.docx, last accessed 5.11.2019.

difficultly of token reproduction. The examples of possession-based authentication factor include (private) asymmetric cryptographic keys, smartcards with stored private asymmetric key, uniquely identifiable token (e.g. a SIM card) or devices with one-time-passwords (e.g. “RSA-Token” or printed cards). Typical attacks on possession-based authentication factors are theft, duplication, and attacks on the process of authentication itself. Inherent authentication factors require the subject to demonstrate a physical attribute of a natural person. The security of this method relies on the fact, that no other person, will have the physical attribute that is identical. The examples of inherent authentication factor include fingerprints, irises, face, voice, palm veins, hand geometry, etc. Behavioural biometrics such as gait or keystroke dynamics can also be used. Typical attacks on inherent authentication factors are spoofing and duplication. By combining multiple factors we get multi-factor authentication, the most common of which is the two-factor authentication, which requires two different factors to be used. A typical combination for two-factor authentication is a password (a knowledge-based authentication factor) and a token received via SMS (a possession-based authentication factor). When using multi-factor authentication, it is a good idea to use different factors, to counter different threats/attack vectors. Dynamic authentication is a type of authentication where the authentication information is different for each session. This is primarily useful for protection against man-in-the-middle attack and various replay attacks.

The field of authentication is primarily relevant in the eIDAS regulation, specifically to electronic identification. eIDAS also specifies different trust levels of identification depending on what security level the e-service wants to achieve. The trust level is primarily determined by how the authentication process is managed and how the identity is issued. eIDAS also defines trust levels (standard, advanced and qualified) for electronic signatures, which are also used for authentication of users. The qualified electronic signature has the same legal value throughout the EU as a handwritten signature.

Authorization establishes if someone (who should already be authenticated) is allowed access to a particular resource. Authorization what someone is and is not permitted to do. Usually authorization is performed with role-based access control (the user is a member of a particular user group), an attribute-based access control (the user has specific clearance) or an access control lists (the user is on the list of approved users).

Access Control is the process of enforcing the required security for a particular resource. After the authentication and authorization has established who the user is and what it is allowed to do, access control prevents the user from doing anything he is not allowed to do. It is a general way of controlling access to resources, including restrictions based on things like the time of day, the IP address of the client, the country of the client, possession of hardware or software tokens, type of encryption they support, etc. A very popular solution for access control is a VPN. VPNs are great at providing authentication but granting different authorization privileges can be difficult.

7.4 Vulnerability Assessment and Penetration Testing

Vulnerability Assessment and Penetration Testing are two types of vulnerability testing. A penetration test attempts to actively exploit weaknesses in an environment. While a vulnerability scan is typically automated, a penetration test requires various levels of expertise. The two tests are designed to find security

vulnerabilities in an organization, but they have different strengths and are often combined to achieve a more complete vulnerability analysis.

A vulnerability assessment is the process of identifying threats and vulnerabilities and measuring their severity. Vulnerability assessments result in a list of vulnerabilities, often prioritized by severity and/or business criticality. Vulnerability assessments typically involve the use of automated testing designed to uncover weaknesses and recommending appropriate remediation or mitigation to remove or reduce risk. In contrast, penetration testing is typically a goal oriented exercise. A penetration test is more focused on simulating a real-life attack, testing defences and mapping-out paths a real attacker could take to fulfil a real-world goal. In other words, a penetration test is usually about how an attacker is able to breach defences and less about specific vulnerabilities. Compared to penetration testing, vulnerability assessment should be a more frequent process, used to continuously monitor and identify weaknesses in an organization and reduce the attack surface. It is a good idea to perform a vulnerability assessment after a leak occurs when a new vulnerability is discovered (with a service, protocol or some other resource that is possibly used in the organization), or if there is a change in the network, an application or service the organization provides. Ultimately, the fundamental difference between vulnerability assessment and penetration testing is the former is list-oriented, while the latter is goal-oriented[111].

Penetration testing is the process of assessing computer systems, networks and applications to identify and address security vulnerabilities that could be exploited. It is an ethical way of "hacking", meant to identify, safely exploits and help to eliminate vulnerabilities in an organisation's defences. A penetration test can be a vulnerability assessment of a particular system or application, a simulation of a real-life cyber-attack to assess the detection and response capabilities of an organization or a replication of a specific attack. When the information about the tested system is provided to the ethical hackers (people who are performing the penetration test) the test is called a whitebox test, while if the attackers are given no information on the system they are attacking (similar to how the attackers in the real world would not have insider knowledge about the system) then the test is called a blackbox test.

There are multiple types of penetration tests, depending on the organization resource that is being tested. Testing configuration of networks, hosts and devices includes an assessment of internal and external network infrastructure designed to test local and cloud based networks, firewalls, system hosts, open ports, weak user credentials, operating systems with latest security updates, the security of remote access to the devices, unsafe user privileges and unpatched applications and devices such as routers and switches [112][113]. Scanning for well-known vulnerabilities is good at identifying basic problems, but human penetration testing is more exhaustive and more likely to uncover vulnerabilities specific to organizations environment

[111] Ian Muscat, The difference between Vulnerability Assessment and Penetration Testing. Published 17.8.2017 at https://www.acunetix.com/blog/articles/difference-vulnerability-assessment-penetration-testing/, last accessed 4.11.2019.
[112] Mike James, What Type of Vulnerabilities Does a Penetration Test Look For? Published 2.12.2018 at https://www.tripwire.com/state-of-security/vulnerability-management/type-vulnerabilities-penetration-test/. Last accessed 4.11.2019.
[113] Redscan, What type of penetration testing does your business need? Published 21.8.2018 at https://www.redscan.com/news/type-penetration-testing-business-need/. Last accessed 4.11.2019.

and circumstances. Network penetration testing is typically divided into internal and external. An internal network penetration test is designed to show the types of attacks and vulnerabilities that a person with access to the internal network (e.g. an employee) could perform and/or exploit. External network test, on the other hand, is meant to test the effectiveness of perimeter security controls (e.g. mail, web, etc.) that an outsider could exploit. An extension of network testing is also the testing of a wireless network. This test helps identify rogue access points, weaknesses in encryption, WPA vulnerabilities etc. Application testing usually includes testing for weaknesses in design, coding and development practices. The testing can be somewhat different for web or mobile applications, but mostly the penetration test checks security of sensitive data that is used, session management and its security, authorization mistakes, data leakage and the security of the communication itself (searching for flaws in encryption and authentication).

7.5 Data availability

There are many possible reasons for data loss (e.g. hardware or software failure, malware, accidents, etc.). To provide continuous operation of the service or at least to reduce the downtime of the service to an acceptable level there have to be contingencies in place for when something going wrong with the stored data, it is important to be able to ensure the data availability. This includes backup, restoration, replication and recovery of data. While at first glance this might seem like a simple problem to tackle, to do it well it should precisely balance multiple variables. What recovery and backup system is used can be determined by the importance of the data, the budget for the system, the cost of the data being unavailable (which should be proportional to how fast we would want the recovery to be), how often to create a recovery point and the speed with which the problematic data should be returned to its original state.

In recent years, the use of cloud technology for the purposes of backing up data has become common. Backing data online in a cloud brings many advantages when compared to the traditional use of tapes or external hard drives. Backing up of data to the cloud can run automatically with minimal effort and the backing can be continuous so that files get backed up as soon as they are changed. This is important to prevent the changes that were made to the data, between the last backup and the data state at the time of failure, to be lost forever. While using your own clod is an option, utilizing a service might be better at also providing off site storage (e.g. in case of a fire at your datacenter). Using a cloud solution also improves the scalability of the system. However, like most things in life cloud storage comes with a few drawbacks as well. When online cloud service is used, the data is not under direct control. There are also cost, performance and security considerations to take into account. Additionally, data is stored in an unknown location (this is also important in the case of the GDPR regulation).

Data availability is one of the most important parts of the service availability. Ultimately, data is very important, but without a system to access the data, it is meaningless. Disaster recovery is a plan for organizations to enable the recovery or continuation of vital technology infrastructure and systems after a catastrophic failure. For large organizations and vital services, this usually involves ‘hot recovery’ provisions involving a shadow side that can take over the operation within minutes of a problem affecting the core operation. For smaller companies, however, this is not a practical or affordable option, but they should have a plan in place to continue working in the event of a major problem, nonetheless. Disaster recovery and in turn the backing up of data is an integral part of the NIS Directive framework.

7.6 Malware protection and antivirus protection systems

Malware protection system is a system designed to detect programs with malicious intent, defend against them and remove malicious software[114]. Antimalware can protect the device in real-time by preventing the installation of suspicious software, by checking the incoming network data and scanning the software. Malware can additionally prevent users from accessing malicious websites and stop the spreading of malware between devices. Antivirus is an older type of protection, designed to protect against more well-known threats (trojan horses, viruses, keyloggers and worms), the kind of threats that do not change or adapt, while antimalware is focused on newer, adaptable threats and zero-day exploits[115].

Antimalware uses different methods to protect the system from malware. First is signature-based detection. The antimalware software (or a server) maintains a list of signatures for every known malicious code. The Signatures are constructed from the features and binary code of individual malware. Antimalware software constructs a signature for each software it is checking and compare the created signature with the list of known malware software. Signature-based detection is good because it is simple to apply and does not use many resources. However, because to recognise a malware, somebody else has had to list the software as such, the signature-based detection is not useful against new malware. Behaviour-based or Heuristic-based detection analyses the behaviour of software before it can execute. Behavior is determined based on parameters such as source or destination address, memory usage, attachments, etc. Modern antimalware software uses machine learning to recognize potentially harmful behavior, based on the previously analyzed behavior of other determinately malicious or non-malicious software. Behaviour-based detection of malware is capable of discovering known threats and threats that were previously unknown. The disadvantage of this type of malware detection is higher complexity (requires more resources) and having to hold large number of behavioural patterns. Specification-based detection each software has its own specified behaviour. The antimalware program monitors the behaviour of the potentially harmful software. If it detects abnormal behaviour it marks the software as malware. Specification-based detection is similar to behaviour-based detection, but it does not require machine learning, because the behaviour is described in the system specification. Consequently specification-based detection is simpler to perform, but not as good as behaviour-based detection, at detecting new threats. A new method the antimalware programs use is sandboxing. Sandbox is an isolated environment, where any new software is run and monitored. If malicious intent is detected by the antimalware software the execution will be terminated and the software flagged as malicious, without causing any harm to the host.

[114] Rabia Tahir, A Study on Malware and Malware Detection Techniques. I.J.Education and Management Engineering, Modern Education and Computer Science Press, 2018, Volume 8, Number 2. DOI: 10.5815/ijeme.2018.02.03. Available at http://www.mecs-press.net/ijeme/.
[115] Margaret Rouse, antimalware (anti-malware), 2017. Available at https://searchsecurity.techtarget.com/definition/antimalware, last accessed 4.11.2019.

8 Summary and conclusion

The comparative analysis of the different legal sources making up the existing EU framework on data protection and cybersecurity confirms the favourable context which characterises the regulatory approach in the European Union. This conclusion is demonstrated by the following table, which compares the results of the analysis of the different regulatory instruments conducted in the previous sections.

It is evident that the GDPR provides a general framework, outlining the main binging principles for the use of data, also in terms of data security. In this sense, the general principles – such as data minimization, storage limitation and data confidentiality – that are defined and stated in this regulation shape the entire regulatory framework.

Furthermore, with regard to these general principles, but also with regard to risk assessment, by-design approach, reporting obligations, and certification process, the GDPR adopts a principles-based approach that is crucial in setting a common paradigm for digital economy. This paradigm is then further elaborated by the other regulations examined here, through a more technology-based and context-specific approach.

In the light of the above and from a business perspective, all the legal provisions exanimated in this analysis, explicitly or implicitly, require the development of specific technologies for cybersecurity and data security, as outlined in Tab. 7. At the same time, the framework provided by these different legal sources is not a patchwork, but a coordinated harmonious model, in which similar technologies are required by different regulations to address issues related to the common core of these regulations. A common core which is based on five main pillars: risk-based approach, by-design approach, reporting obligations, resilience, and certification schemes.

This uniformity demonstrates the existence of a *fil rouge* that characterises the whole approach adopted by the EU legislator in the field of data protection and cybersecurity, and undoubtedly provides a clear and unique framework for the development of a roadmap for the implementation of the Network of Competence Centres.

Table 7: Common core

Rules and principles	**GDPR**	**PSD2**	**eIDAS**	**NIS**
Data minimization	Systems and services that minimise data collection and use of personal data			
Data storage limitation	• Data retention limitations • Pseudonymisation • Encryption • Access control			

	• Server and data base security • Network and communication security • Automatic periodic data deletion			
Data confidentiality	• Security policies • Records of processing activities • Physical security			
Risk assessment and security measures	• Risk analysis • DPIA • Technical and organisational measures	• Operational and security risk management framework • Control model • Physical security • Access control • Continuous monitoring and detection	• Use of authentication factors (Knowledge-based factors, possession-based factors, private keys) • Use of inherent factors	• Communication (email) risk assessment (Domain Keys Identified Mail, Sender Policy Framework, Domain-based Message Authentication, Reporting and Conformance) • Software management • Access control • Authentication factors
Data protection by design and by default	• Adoption of specific security requirements and procedures since the early stages of the development lifecycle • Procedures to integrate data protection safeguards into processing activities • Specific technologies able to support privacy and data protection (PETs)	Secure technologies by design and by default (data minimisation, pseudonymization, encryption, privacy-oriented users' profiles settings)	Use a catalogue of specific design patterns to develop solutions to known security problems	
Regular assessment of	• Records of the adopted technical			

the effectiveness of the security measures adopted	and organisational security measures • Vulnerability and penetration testing (e.g. vulnerability scanning; ethical hacking)			
Notifications, reporting obligations, and mitigation measures **(data breaches)**	• Appropriate procedures to establish immediately whether a personal data breach has taken place • Incident response plan • Data flow and log analysers • Tokenization; encryption, etc.	• Early warning indicators • Pocesses and organisational structures to ensure the consistent and integrated monitoring, handling and follow-up of operational or security incidents • Procedure for reporting	Different forms of notification	Mandatory report to the National Agency in case of significant disruptions • Adopt alerting systems • Information collection on incident • Provide information on security issues • Automatizations of notification systems
Business Continuity, Disaster Recovery, and Resilience	• Business continuity plan • Data restore procedures • Adoption of an effective "cyber resilience" approach • Disaster recovery plan • Backup techniques • Technological measures to ensure business continuity	• Identify a range of different scenarios • Develop response and recovery plans	• Business impact analysis and a threat analysis • risk assessment • recovery time • risk management, vulnerability management, identification and prioritization of business processes and supporting applications, etc.	• Cyber-resilience and business continuity Cyber risk and vulnerability management • Incident response team • Alternative resources to use in case of crisis • Back- up systems
Certification process		• No specific requirements for certification or default industry standards • No national authority requires such certification processes at present • The EBA is not mandated to make certification processes compulsory	Qualified electronic signature creation devices (QSCD certification) and qualified trust services provider (QTSP supervision).	

		• The alternative of market-driven certification processes is voluntary, the EBA has concluded that there is little subject matter that could conceivably be harmonised through EBA Guidelines.		
Annual report to the European Authority		• Record data from all agents and aggregate data • Statistical reporting systems	• Application or software open source to report easily and readily • Technologies capable to classify annual incidents • Set of capabilities to create cluster for sectors and industries.	• Resource to assist in successfully handling information necessary for the report • Channels with strong authentication to collect and store data about incidents required to fill the report • Structural support to target and seclude data and information about incidents • Secure channel to share information with the Commission

References

EBA. 2017. Final Report on Guidelines on Security Measures for Operational and Security Risks under PSD2. Available at https://eba.europa.eu/sites/default/documents/files/documents/10180/2060117/d53bf08f-990b-47ba-b36f-15c985064d47/Final%20report%20on%20EBA%20Guidelines%20on%20the%20security%20measures%20for%20operational%20and%20security%20risks%20under%20PSD2%20(EBA-GL-2017-17).pdf, last access 2 November 2019.

EBA. 2018. Guidelines on fraud reporting under PSD2. Available at https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-fraud-reporting-under-psd2, last access 2 November 2019.

Article 29 Data Protection Working Party, Statement on the role of a risk-based approach in data protection legal frameworks, adopted on 30 May 2014, WP218. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf, last access 2 September 2019.

Article 29 Data Protection Working Party. 2014. Opinion 5/2014 on Anonymisation Techniques, WP216.

Article 29 Data protection Working Party. 2014. Opinion 5/2014 on Anonymisation Techniques, WP216, adopted on 10 April 2014. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm, last access 5 September 2019.

Article 29 Data Protection Working Party. 2017. 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. Adopted on 4 April 2017, as last revised and adopted on 4 October 2017, WP 248 rev.01. Available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236, last access 2 September 2019.

Article 29, Data Protection Working Party. 2018. Guidelines on Personal data breach notification under Regulation 2016/679, adopted on 3 October 2017, as last revised and adopted on 6 February 2018, WP250rev.01. Available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052, last access 2 September 2019.

Barrinha, A., and Farrand-Carrapico, H. 2018. How Coherent is EU cybersecurity policy? in EUROPP – European Polictics and Policy - available at https://blogs.lse.ac.uk/europpblog/2018/01/16/how-coherent-is-eu-cybersecurity-policy.

Cavoukian, A. 2010. Privacy by design: the definitive workshop. A foreword. 3(2) IDIS 247-251.

Cranium Campus, Summary of Privacy Enhancing Technologies – A Survey of Tools and Techniques. Available at https://craniumcampus.eu/summary-of-privacy-enhancing-technologies-a-survey-of-tools-and-techniques/, last access20 September 2019

Dewitte, P. 2018. Email me not: direct marketing, GDPR and ePrivacy Regulation. Available at https://www.law.kuleuven.be/citip/blog/email-me-not-direct-marketing-gdpr-and-eprivacy-regulation/, last accessed 5 December 2019.

DQM GRC confidence in data, Essential Security Technologies for GDPR. Compliance, available at https://www.dqmgrc.com/file/785/download?token=KuAoDE6C, last access 5 December 2019.

EDPB. 2018. Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications. Available

at https://edpb.europa.eu/our-work-tools/our-documents/drugi/statement-edpb-revision-eprivacy-regulation-and-its-impact_en, last accessed 5 December 2019.

EDPB. 2019. Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. Available at https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf, last accessed 5 December 2019.

ENISA. 2016. Guidelines for SMEs on the security of personal data processing. Available at https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing, last access 5 September 2019, 45.

ENISA. 2016. PETs Controls Matrix report. Available at https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-privacy-tools, last accessed 2 November 2019.

ENISA, 2017. Handbook on Security of Personal Data Processing. Available at https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing, last access 30 September 2019.

ENISA. 2018. Recommendations on shaping technology according to GDPR provisions. An overview on data pseudonymisation. Available at https://www.aepd.es/media/docs/recomendations-on-shaping-technology-according-to-GDPR-provisions-2.pdf, last access 5 September 2019.

ENISA. 2019. Recommendations on shaping technology according to GDPR provisions. An overview on data pseudonymisation. Available at https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions, last accessed 8 October 2019.

European Commission, Guidance for the application of the levels of assurance which support the eIDAS Regulation. Available at https://ec.europa.eu/cefdigital/wiki/download/attachments/40044784/Guidance+on+Levels+of+Assurance.docx, last accessed 5 November 2019.

European Data Protection Supervisor. 2018. Opinion 5/2018. Preliminary Opinion on privacy by design. Available at https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf, last access 1 September 2019.

European Union Agency for fundamental rights (FRA). 2018. Handbook on European data protection law. Available at https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law, last access 5 September 2019.

Hadlington, L. 2018. The “Human Factor” in Cybersecurity: Exploring the Accidental Insider. In McAlaney, J., Anne Frumkin, L., Benson, V. Psychological and behavioral examinations in cyber security. Hershey, PA IGI Global.

IAB. 2018. IAB Europe Position on the proposed ePrivacy Regulation. Available at https://iabeurope.eu/wp-content/uploads/2019/10/31.10.2018-IABEU-ePR_Position_Paper.pdf, last accessed 5 December 2019.

Information Commissioner’s Office – ICO, Data protection by design and default. Available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/, last access 2 September 2019.

Information Commissioner's Office in the United Kingdom. Available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/, last accessed 3 November 2019.

James, M. 2018. What Type of Vulnerabilities Does a Penetration Test Look For? Available at https://www.tripwire.com/state-of-security/vulnerability-management/type-vulnerabilities-penetration-test/, last accessed 4 November 2019.

London Economics. 2010. Study on the economic benefits of privacy-enhancing technologies (PETs). Available at https://londoneconomics.co.uk/wp-content/uploads/2011/09/17-Study-on-the-economic-benefits-of-privacy-enhancing-technologies-PETs.pdf, last accessed 4 November 2019.

Long, RM., Blythe, F., Raul, A. C. 2018. European union overview. In Raul, A.C. (ed), Privacy, Data Protection and Cybersecurity law Review. The Law Reviews, 5th edition

Mantelero A. Forthcoming. Comment to Article 35 and 36. In Cole, M., Boehm, F. (eds.). GDPR Commentary, Edward Elgar Publishing.

Mantelero, A., Vaciago, G. 2017. Legal Aspects of Information Science, Data Science and Big Data. In Dehmer, M., Emmert-Streib, F. (eds). Frontiers in Data Science. (CRC Press).

Menze, T. 2019. The State of Industrial Cybersecurity. Available at https://ics.kaspersky.com/media/2019_Kaspersky_ARC_ICS_report.pdf.

Muscat, I. 2017. The difference between Vulnerability Assessment and Penetration Testing. Published. Available at https://www.acunetix.com/blog/articles/difference-vulnerability-assessment-penetration-testing/, last accessed 4 November 2019.

Prodan, M., Prodan, A., Purcarea, A.A. 2015. *Three New Dimensions to People, Process, Technology Improvement Model*. Polytechnic University of Bucharest.

Redscan, What type of penetration testing does your business need? Available at https://www.redscan.com/news/type-penetration-testing-business-need/, last accessed 4 November 2019.

RM Long W., Scali G., Blythe F., Raul A. C., European union overview, in Privacy, Data Protection and Cybersecurity law Review, 2018, 5th edition.

Rouse, M. 2017. Antimalware (anti-malware). Available at https://searchsecurity.techtarget.com/definition/antimalware, last accessed 4 November 2019.

Tahir, R. 2018. A Study on Malware and Malware Detection Techniques. I.J.Education and Management Engineering, 8(2) Modern Education and Computer Science Press. DOI: 10.5815/ijeme.2018.02.03. Available at http://www.mecs-press.net/ijeme/, last accessed 4 November 2019.

The Office of the Privacy Commissioner of Canada. 2017. Privacy Enhancing Technologies – A Review of Tools and Techniques. Available at https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711, last accessed 2 November 2019.

The Royal Society. 2019. Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis. Available at https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies/, last accessed 2 November 2019.

Voss, G. 2017. First the GDPR, now the proposed ePrivacy Regulation. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3008765, last accessed 5 December 2019.

Zuiderveen Borgesius, F.J.; Kruikemeier, S.; Boerman, S.C.; Helberger, N. 2017. Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation. Available at https://www.ivir.nl/publicaties/download/EDPL_2017_03.pdf, last accessed 5 December 2019.