HELLENIC REPUBLIC
National and Kapodistrian University of Athens
EST. 1837

LAW SCHOOL

POSTGRADUATE PROGRAM: LL.M. in International and European Law
SPECIALIZATION: European Law
ACADEMIC YEAR: 2023 - 2024

POSTGRADUATE THESIS

Anastasia Vasiliki Tsilivakou

R.N.: 7340202302020

"Examining the interplay between the GDPR and NIS 2 Directive in shaping a secure European digital landscape"

Supervisors:

a) Associate Professor Rebecca-Emmanuela Papadopoulou (Supervisor)

b) Associate Professor Manolis Perakis

c) Assistant Professor Metaxia Kouskouna

Athens, September 2024

Table of Contents

List of Abbreviations

APWG - Anti-Phishing Working Group

AR-in-a-BOX - Awareness Raising in a Box

CER Directive - Directive on the resilience of critical entities

CJEU - Court of Justice of the European Union

Charter – Charter of Fundamental Rights of the European Union

EC – European Commission

EC^3 - European Cybercrime Centre

ECSM - European Cybersecurity Month

EMSA - European Maritime Safety Agency

ENISA – European Union Agency for Cybersecurity

EU – European Union

GDPR – General Data Protection Regulation

ICT systems – Information and communication technology systems

IoT – Internet of Things

NIS Directive – Directive on Security of Network and Information Systems

NIS 2 Directive – Directive on Security of Network and Information Systems 2

OECD – Organisation for Economic Cooperation and Development

PETs – Privacy-enhancing technologies

SCCs – Standard Contractual Clauses

SDL – Microsoft's Security Development Lifecycle

SMEs - Small and Medium-Sized Enterprises

TEU – Treaty on European Union

TFEU – Treaty on the Functioning of the European Union

To my family, with deep gratitude for their love and support,

and in loving memory of my grandmother.

PREFACE

'*The Web as I envisaged it, we have not seen it yet. The future is still so much bigger than the past.'*

This is a famous quote by Sir Timothy John Berners-Lee, an English computer scientist and most notably the father of the World Wide Web and other technological inventions as the URL system and the HTTP, which shaped the internet and the world alongside of it.

The evolution of the internet from the 1990s to the 2020s marked a period of rapid and intense technological growth and transformation. In 1991, Tim Berners-Lee introduced the World Wide Web to the public, revolutionizing how people perceived and shared information, laying the foundations for the modern internet. A few years later, the web would become more accessible to the general public, and by the late 1990s the emergence of e-commerce platforms like *Amazon* and *eBay*, marked the beginning of online retail, enhancing the online experience.

By 2004, the founding of *Facebook* signaled the rise of social media, transforming how people communicated and shared information. The launch of *YouTube* in 2005 changed the landscape of artistic creation, sharing, and most specifically consumption. In 2007, *Apple's* release of the iPhone revolutionized the mobile phone industry, making smartphones essential digital devices. The 2008 launch of the Android operating system provided a less constly alternative to *Apple*'s iOS, fueling the growth and sales of mobile apps and the broader mobile technology. During this time, cloud computing gained traction with services like *Amazon Web Services*, enabling effective and flexible IT infrastructure. The 2010s saw the rise social media platforms such as Twitter, Instagram, and Snapchat, which gained massive popularity, further establishing social media in daily life. In 2011, *IBM's Watson*, an AI system capable of answering questions in simple and natural language, marked significant progress in artificial intelligence. The mid-2010s saw the emergence of the 'Internet of Things', connecting everyday devices to the internet and enabling 'smarter' daily lives, through 'smart homes', 'smart cities', resulting in further establishing the tech industry in terms of supply.

And then the clock stopped in 2020. And when it started ticking again, it did so fiercely. The COVID-19 pandemic acted as a catalyst, accelerating the emergence of new technologies and the digital transformation across various sectors. Remote work became the norm, with businesses relying heavily on digital collaboration tools and cloud computing for their services and to maintain operations, while online education saw immense growth as schools and universities moved their curricula online. E-commerce also experienced a significant boom, driven by the need for contactless shopping, leading to innovations in logistics and delivery services. In 2021, the concept of the metaverse gained substantial fame, particularly with *Meta* (formerly Facebook) leading its development. The metaverse envisions a fully immersive and interconnected digital world, where people can work, socialize, and create, through the establishment of virtual and augmented reality technologies. The idea of the metaverse has the potential to revolutionize a lot of sectors, from entertainment and gaming to real estate and education. Ongoing advancements in artificial intelligence, machine learning, blockchain, and cloud computing are continuously driving innovation, shaping the future of digital technology. AI and machine learning are increasingly

integrated into industries like healthcare, finance, and marketing, boosting productivity and enabling new levels of automation. Blockchain technology is also expanding beyond cryptocurrencies, with promising applications in supply chain management and digital identity verification.

However, as it can be understood from the brief history of the digital world, no matter how extraordinary the journey of the internet has been, these new technological inventions, impose important questions about digital identity and privacy. From its humble beginnings to its stable establishment in our daily lives, it has transformed the way we communicate, learn, and interact.

But as we look ahead, the question remains: What will the next decade bring and will we be prepared to face the new challenges that come alongside of it?

And Sir Timothy John Berners-Lee was in fact right; the Web as he envisaged it, we have not seen it yet; or perhaps we are now starting to have a brief glimpse of it.

INTRODUCTION

The digital revolution—rather than digital transformation, as the word 'transformation' implies a gradual change or development, whereas the word 'revolution' contains the notion of rapid and disruptive change and therefore seems more appropriate — as thoroughly analysed above in the form of '*a brief history of the internet*' could not come without its risks or challenges. The abundance of online activities, with which individuals can associate themselves has undoubtedly led to a high risk of cyberattacks, data breaches and identity theft, making the protection of personal data and sensitive information online a critical concern. As both public and private organizations embrace new technologies and digitize their operations or services, addressing cybersecurity threats has become a significant challenge and a necessary requirement.

Parallel to the emergence of digital activities and opportunities, the vast amounts of data generated by online activities have raised concerns about how personal information is collected, used and shared by companies and public organizations. Privacy is deemed as a crucial aspect of the digital revolution, as the increased reliance on technology and data collection can infringe individual privacy and rights deriving thereof.

In recent years, this digitization has made data security a pressing concern, especially in context of the European Union, where the regulatory landscape is reliable, but still evolving. European legislation has made fast and robust steps in building digital security through legislative measures such as the General Data Protection Regulation (hereinafter the 'GDPR') in 2016 and the Network and Information Security (hereinafter the 'NIS') Directive and its reform, the Network and Information Security 2 Directive (hereinafter the 'NIS 2'). These legislative initiatives aim to ensure the protection of personal data and enhance cybersecurity in the Union

respectively. Although there are other legislative measures that help with digital security in the Union, data protection and cybersecurity are always examined together, as they are often referred to in academic literature as '*the two sides of the same coin'*.

Given the close connection of data protection and cybersecurity, this thesis explores the possible ways of forming an environment of digital security in Europe by the intersection of the GDPR and NIS 2, focusing on two main aspects: the reinforcement of data protection principles under the GDPR and the enhancement of cybersecurity measures, in light of the revised NIS 2 Directive. The analysis mainly focuses of the examination of legal obligations deriving from both the GDPR and NIS 2 Directive in applying appropriate organizational and technical safeguards, which aim at enhancing security. The GDPR mandates that suitable technical and organizational strategies must be applied and integrated into the processing activities to fulfill the requirements of data protection rules and safeguard the rights of data subjects. NIS 2 Directive on the other hand, imposes the obligation for the adoption of proportionate technical, operational and organisational measures to mitigate the risks posed to the security of network and information systems, which are used for operation or for the provision of services. It is evident from the above, that businesses have legal obligations to implement appropriate technical measures under both the GDPR and NIS 2, but their clear lines and objectives of these obligations are somehow blurry. One can only wonder to what extent these obligations collide, how they can be achieved in practice and how their interplay can foster digital security in Europe.

When examining the practical application of these legal obligations, it is important to simultaneously cover how they interact and influence each other. This will be researched upon in the light of how GDPR's data protection principles and privacy by design interact with cybersecurity, and on the other hand, how cybersecurity measures can contribute to the protection of personal data. In order to review and evaluate how these frameworks work together to strengthen Europe's digital security, Chapter A of Part I of this thesis addresses the reinforcement of GDPR's principles, which emphasize the impact of data processing rules and the integration of privacy principles into system development. Additionally Chapter B, delves in great detail into the concept of cybersecurity and its application in IT systems, as well as notions like cyber hygiene and cyber resilience, which are critical for protecting personal data, but are surrounded by big ambiguity.

In opposition, the application of both the GDPR and NIS2 Directive has shown some hidden shortcomings, which may not be obvious at a first glance, therefore Part II examines the broader challenges and limitations of digital security in Europe. After these challenges are examined and clearly stated, potential solutions will be sought to address them. In this Part, Chapter A will be assessed under the light of European legislation and most specifically how EU's competence and the principle of conferral may limit the scope and uniform application of cybersecurity measures. Furthermore, the introduction to a new right to cybersecurity will be assessed as a possible solution to this shortcoming. In parallel, Chapter B investigates the challenges faced by small and medium-sized enterprises (hereinafter 'SMEs') in maintaining adequate levels of cyber awareness, and the tension between market forces and compliance with GDPR rules, for which EU funding will be explored as a potential remedy for these limitations.

Ultimately, this research, at the same time, aims to provide a comprehensive analysis of the Union's current digital security framework, with a focus on the interplay between legislative

measures and the practical implementations of them, concerning cybersecurity and data protection under the GDPR and NIS 2 Directive. However, the scope of this research will not extent to analyzing the GDPR and NIS Directive on their entirety, but it will mainly focus on the articles that impose an obligation for the adoption of technical safeguards. The fast passed nature of digital threats, mostly cyberattacks and data breaches, calls for a proactive approach to legislation and enforcement. Thus, continual adaptation and enhancement of regulatory frameworks seems vital, taking also into account that apart from the current innovations, technological advancements occur constantly and new challenges arise.

Finally, this research is made under the umbrella of the need for strong regulatory actions that protect individuals' rights, while at the same time encouraging trust in the digital world and new technological innovations. Its aim seek to also identify potential areas for improvement of the current regulatory framework, ensuring its effectiveness and relevance in addressing the challenges and threats of the modern digital world. As a last note, research findings and opinions will be discussed in the conclusion of this thesis, where it will also be assessed if the current framework is effective.

PART I: ENHANCING DIGITAL SECURITY IN THE EUROPEAN UNION

1. An Overview of the Historical Development of the General Data Protection Regulation

Before unraveling the hidden similarities and interplay of data protection and cybersecurity through the GDPR and NIS 2 Directive, it is crucial to first analyse the reason for their adoption, along with their scope and objective, through a brief historic overview.

Starting with the GDPR, the organized efforts for the development of a specific data protection framework started around the 1980's, when the use of the internet was rapidly increasing and new innovations on the field were inevitable. In this time there was, also, a growing concern about the potential for misuse of personal data. It was at that time when the Organisation for Economic Cooperation and Development (hereinafter the 'OECD') issued guidelines for the protection of personal data and transborder data flows.[1] The guidelines were intended to help countries develop national data protection policies and to promote international cooperation in this area, while they managed to establish a global standard for privacy and data protection. Since then, they are consistently cited in the evolution of data protection and privacy laws worldwide and serve as the foundation for many national frameworks.[2] A year later, and more specifically in 1981,

[1] OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [1980] OECD/LEGAL/0188.

[2] Report on the Implementation of the OECD Privacy Guidelines' (OECD, 8 November 2023) <https://www.oecd.org/en/publications/2023/11/report-on-the-implementation-of-the-oecd-privacy-guidelines_f13a77a2.html> accessed 26 August 2024.

the Council of Europe adopted the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data[3], commonly referred to as Convention 108. Under Convention 108, the parties were required to take all necessary steps in their domestic legislation, in order to apply the principles laid down therein, with the ultimate goal to ensure respect in their territory for the basic human rights of all individuals with regard to processing of personal data.[4] The revised version of the text, Convention 108+, was drafted many years later and more specifically in 2018, making it the legal standard for data protection in Europe.[5]

Nonetheless, as it is clear both the Guidelines of the OECD, as well as the Convention 108 did not provide for a comprehensive protection framework for individuals or establish consistent data protection standards across the territory of the European Union (hereinafter the 'EU'). And we are discussing about a protection framework for individuals, because data protection was primarily concerned about safeguarding the rights and interests of individuals, rather than focusing solely on the data associated with them.[6]

To address these shortcomings and facilitate the free flow of information within the EU, the Data Protection Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive 95/46/EC)[7] was introduced and adopted (hereinafter the 'Directive'). The Directive would address the inconsistency caused by the absence of an EU instrument, which could restrict the free movement of people and services and therefore data, ultimately undermining the development of the internal market.[8] As a Directive, it required the EU Member States to adopt their own national laws that implemented the Directive's provisions, leaving them flexibility in the specific means and methods used to achieve the objectives deriving from it. In practice, this means that different enforcement methods and types of sanctions would apply simultaneously in the Member States. Therefore, with regard to the harmonization of data protection measures all of the above-mentioned measures were insufficient in providing sufficient protection for individuals and failed to ensure the harmonization of data protection policies across the European Union due to its legal nature.

The response to the lack of harmonization and uniform application of data protection rules within the EU would come some years later following massive restructures in the EU's legal structure due to the Treaty of Lisbon in 2009. More specifically, the right to data protection was introduced in Article 16 of the Treaty on the Functioning of the European Union (hereinafter the 'TFEU'), which provided (and still does) that '*Everyone has the right to the protection of personal data concerning them*'[9]. The most important aspect of Article 16 TFEU, though, lies with the fact

[3] Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data [1981] ETS 108.
[4] Convention 108 and Protocols - Data Protection - Www.Coe.Int' (*Data Protection*) <https://www.coe.int/en/web/data-protection/convention108-and-protocol> accessed 26 August 2024.
[5] Ibid.
[6] Hustinx Peter, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation'.
[7] Directive 95/46/EC of the European Parliament and of 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 [1995] OJ L281/31.
[8] Hustinx Peter, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' page 9.
[9] Article 16 par. 1 of the consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47.

that it served as a legal basis for the adoption of secondary legislation on data protection.[10] Additionally, the Charter of Fundamental Rights of the European Union (hereinafter the 'Charter') was advancement to the status of EU primary law, equal to the EU Treaties. And that is particularly important given that the Charter included a specific right to data protection in Article 8, which provided that all individuals have the right to the protection of personal data concerning them, which must be processed fairly for specified purposes based on the individual's consent or another legitimate legal basis.[11] Established years after the Data Protection Directive, Article 8 of the Charter embodies the existing EU data protection framework, by not only explicitly recognizing the right to data protection in paragraph 1, but also by outlining core data protection principles in paragraph 2. Ultimately, the Charter elevated data protection to the status of a fundamental right under EU law and all of EU institutions and Member States, when applying Union law[12], are required to protect and respect this right. Article 7 of the Charter, also, guaranteed the respect for private and family life.[13] The difference between privacy and data protection will be analysed and explained thoroughly in the next Chapter.

Following these revolutionary developments in the EU's structure and legal framework, the Commission recognized in 2010 the need to reform data protection measures derived from the Directive, in response to globalization and emerging technological advancements[14]. In November 2011 the first draft for the General Data Protection Regulation (hereinafter the 'GDPR') was circulated internally within the Commission by the Directorate General for Justice and in January 2012 the draft proposal was published by the Commission[15], followed by a not so welcoming political reaction.[16] After four years of negotiations and amendments to the initial draft of the Commission, the Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (Regulation 2016/679/EU)[17] was adopted in April 14, 2016, repealing Directive 95/46/EC and entered into force on 25 May 2018, following a two year implementation period.[18]

The whole mindset surrounding the adoption of the GDPR revolved around the fact that individuals should retain control over their personal data and legal certainty should be improved for individuals, businesses, and public authorities, due to the rapidly changing technological

[10] Ibid para. 2.
[11] Article 8 of the European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.
[12] Ibid Article 51.
[13] Ibid Article 7.
[14] 'Background and Evolution of the EU General Data Protection Regulation (GDPR) | The EU General Data Protection Regulation (GDPR): A Commentary | Oxford Academic' <https://academic.oup.com/book/41324/chapter-abstract/352293200?redirectedFrom=fulltext> accessed 27 August 2024.
[15] Donnees personnelles, 'A General Data Protection Regulation For Europe? Light And Shade In The Commission's Draft Of 25 January 2012' [/01/23] SCRIPTed <https://script-ed.org/?p=406> accessed 27 August 2024.
[16] In Germany, *Johannes Masing*, a judge of the German Federal Constitutional Court (*Bundesverfassungsgericht*), expressed criticism and concerns about the proposed regulation, arguing that due to the primacy of EU law national provisions on data protection would stop to be applicable, leading to the limitation of the jurisdiction of the national constitutional courts accordingly.
[17] 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) [2016] OJ L119/1
[18] Background and Introduction to the General Data Protection Regulation (*Lexology*, 19 September 2017) <https://www.lexology.com/library/detail.aspx?g=d7f59709-4362-4155-ab6f-de55af4147a4> accessed 27 August 2024.

landscape.[19] These changes were in a desperate need of a strong and cohesive data protection framework across the EU, which would result in building trust in the digital economy.

Having used Article 16 TFEU as the legal basis and adopted according to the ordinary legislative procedure, the GDPR affirmed the goals and principles of Directive 95/46/EC[20], and aimed to prevent fragmentation in data protection implementation across the Union and legal uncertainty. Due to its legal nature, the GDPR provides for uniform application resulting from its direct applicability across all EU Member States and hence removes barriers to data flows that could arise from differences in national laws, thereby achieving its primary goal of facilitating the free movement of personal data within the EU. In this regard, GDPR 'pre-empts' existing national data protection laws, although it does allow Member States to adopt certain additional legal measures[21], such as enhancing the authority of national data protection authorities.

The Regulation contains 99 Articles and is five times longer than the Directive. With a view to explaining the primary aim of expanding the regulatory framework, it is imperative to highlight the need to enhance the protection afforded to data subjects by setting stricter time limits on data storage[22], extending the territorial scope to cover cases where processing occurs outside the Union[23], and introducing heavier penalties for specific infringements.[24] At the same time, it increased the legal certainty needed for the smooth conduct of economic activities that rely on digital technology.

Additionally, the Regulation emphasizes a proactive approach rather than a reactive one by requiring data controllers to ensure, even from the phase of design of the collection and processing method, that technical measures are taken into consideration and are being implemented[25], in order to maintain an appropriate level of security against the risks posed by new technological developments. This is the so called *privacy by design*, which will be analysed thoroughly in this chapter. In particular, this approach emphasizes the importance of the '*technocratic'* component[26] in the effective management of data, more than the purely legal or administrative one. A key innovation in this regard is the introduction of impact assessments for the evaluation of potential risks, as well as the assessment of safeguards and protection measures. This technocratic perspective applies to the entirety of the Regulation: from the obligation to keep pace with technological developments, to ensuring the reliability of processors and adherence to specific codes of conduct or certification.

In this way, the legal protection of data and issues, such as the lawfulness of processing or liability in the event of infringement, are fundamentally linked to technical compliance[27], including the degree to which specific specifications have been followed or the actual consequences of non-compliance. This proactive approach ensures that security is embedded within systems, rather than

[19] Peter Chase, 'Perspectives on the General Data Protection Regulation Of the European Union'.
[20] Regulation (EU) 2016/679 Recital 9.
[21] Ibid Recital 10.
[22] Article 5 para. 1 (e) of Regulation 2016/679.
[23] Article 3 para. 2 and 3 of Regulation 2016/679.
[24] Article 83 para. 4, 5 and 6 of Regulation 2016/679.
[25] Article 25 para. 1 of Regulation 2016/679.
[26] Fereniki Panagopoulou-Koutnatzi, 'The General Data Protection Regulation (EU) 679/2016: Introduction and Fundamental Rights Protection' (Sakkoulas, 2017) (translated in English).
[27] Ibid.

being added after the occurrence of an incident of a data breache. This is crucial for mitigating risks associated with evolving cyber threats and therefore, this exact perspective will be examined in the context of its link to cybersecurity.

2. Historical Overview of the Evolution of NIS 2 Directive

With regard to the second piece of secondary legislation that will be analysed and in the context of cybersecurity, the first efforts to create a legislative framework in Europe started with the United Nations Convention on Cybercrime in 2001[28], due to the rapid digitalization and the dangers posed by the potential misuse of computer networks and electronic information for criminal activities. The Convention in Cybercrime prioritized the development of a uniform criminal policy focused on protecting society from cybercrime, including the adoption of legislation and the promotion of international cooperation and therefore making these its main objective, as set out in its preamble. It also targeted the harmonization of national criminal legislation, in terms of offenses and their link to cyber crime, while providing for procedural elements for the prosecution of such offenses.[29] Of great importance to the writing of this thesis is the fact that the Convention directly affirmed the right to the protection of personal data, as conferred in Convention 181.[30]

Following Convention 185, concentrated efforts to build a cybersecurity framework within the EU started with the EU Cybersecurity Strategy in 2013, as outlined by the European Commission (hereinafter the 'EC') together with the High Representative of the Union for Foreign Affairs and Security Policy[31]. The Strategy came as a result of the internet and cyberspace having influenced and impacted society and daily life, as well as fundamental rights and the economy. With regard to economy, information and communication technologies had become essential in various sectors and digital economy was vital for economic growth.[32] In this context the EC understood that in order to keep cyberspace open and secure, the principles of democracy, fundamental rights and the rule of law that applied offline would also have to apply online. This would be achieved through the establishment of cybersecurity measures and the preserving of the reliability of the Internet, given the immense impact of cybersecurity incidents in the economy and fundamental rights. As a result, the Strategy set out a vision for a secure cyberspace, identified key priorities and actions for achieving cyber resilience, reducing cybercrime, building cyberdefence and promoting international cooperation in cyberspace. Nonetheless, the most important element

[28] Council of Europe, Convention on Cybercrime [2001] ETS 185.
[29] Ibid Article 13.
[30] Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data [1981] ETS 108.
[31] European Commission, and High Representative (2013) Cybersecurity strategy of the European Union: an open, safe and secure cyberspace.
[32] Ibid Introduction to the Cybersecurity Strategy

of the Strategy was a proposal for a Directive on network and information security (NIS Directive)[33].

The Directive on Security of Network and Information Systems (hereinafter the 'NIS Directive') was adopted on 16 July 2016, providing for a two-year period transposition ending on 9 May 2018[34], and its subject matter and scope was '*achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market'*[35]. The NIS Directive focused on three main aspects: *a)* ensuring Member States are prepared to address a cyber-incident through adopting national security measures and the establishment of a national supervision NIS authority, *b)* fostering cooperation between Member States through a 'Cooperation Group'[36] and a 'CSIRT Network'[37] and *c)* building a 'culture' of security of vital sectors.[38] In essence, NIS Directive had a limited scope; it imposed cybersecurity obligations only to a specific group of actors, such as operators of essential services and digital service providers.[39] In fact, businesses that had a vital role for the society and economy, such as the sector of energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure had to be identified as such by the Member State[40] and would undertake the obligation to take appropriate security measures and to notify serious cyber-incidents to the relevant national authority[41].

In addition, key digital service providers, such as search engines, cloud computing services and online marketplaces had also an obligation to comply with the security and notification requirements under the NIS Directive.[42] Additionally, it was decided that the criterion for a uniform application should be established, according to which all entities would fall within the scope of application of this Directive based on their size. Specifically, all medium and large enterprises, as defined by Commission Recommendation 2003/361/EC[43], that operate within the above-mentioned sectors or provide the type of services covered by NIS Directive would all fall within its scope with no additional actions required on the part of Member States. On the contrary,

[33] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) [2016] OJ L 194.
[34] Ibid Article 25.
[35] Ibid Article 1.
[36] The Cooperation Group's tasks involved providing guidance for the CSIRTs Network, assisting Member States in adopting appropriate measures, also through the support in the identification of operators of essential services, engaging with relevant EU institutions and bodies and evaluating national NIS strategies.
[37] Computer security incident response teams (CSIRTs). Their tasks included mainly the exchange of information on CSIRT services and operations, discussing incidents and coordinating responses and supporting cross-border incident handling. The CSIRTs had the obligation to inform the Cooperation Group of their activities and seek guidance when needed.
[38] EU Cybersecurity Initiatives: Working towards a More Secure Online Environment | Shaping Europe's Digital Future' (5 July 2016) <https://digital-strategy.ec.europa.eu/en/library/eu-cybersecurity-initiatives-working-towards-more-secure-online-environment> accessed 1 September 2024.
[39] Designation of Operators of Essential Services – CSSF <https://www.cssf.lu/en/2020/10/designation-of-operators-of-essential-services/> accessed 2 September 2024.
[40] Article 5 of Directive (EU) 2016/1148.
[41] Ibid Article 14.
[42] Ibid Article 16.
[43] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises [2003] OJ L 124

for micro and small entities, the Member States would have to decide which ones fall within the scope of NIS Directive and then notify the Commission.

A high level of criticism has been expressed with regard to the scope of NIS Directive, due to the fact that according to Article 1 '*this Directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market,* in a sense that it was the functioning of the internal market that NIS Directive intended to safeguard, and not the rights of natural and legal persons. It is evident that the legal basis for the adoption of NIS was Article 114 TFEU, which provides the EU with the authority to adopt legislative measures that contribute to the establishment and functioning of the internal market, while harmonizing legislation within the Member States when differences or discrepancies between national laws can impede the operation of the internal market. The idea behind the use of Article 114 TFEU as the legal basis for NIS Directive was because cybersecurity threats and incidents could severely disrupt the operation of essential services and affect cross-border activities, resulting in obstructing the internal market's smooth functioning. A thorough analysis of the EU's competence and its implications in the adoption of cybersecurity related legislation will be examined later on in Part II. Having taken the above into consideration, the NIS Directive does not grant any protection to individuals or entities whose rights may be violated, if the parties responsible under the Directive fail to fulfill their legal obligations. If cybersecurity issues arise due to non-compliance with the NIS Directive, those impacted by such breaches are not empowered to take any action.[44]

These very first steps in building a secure cyber environment within the EU were violently disrupted by two major cyber-attacks, perhaps the biggest Europe has even experienced; the WannaCry attack and Petya attack both taking place in 2017. WannaCry attack disrupted more than 230.000 computers by encrypting files and demanding a ransom in Bitcoin for their release[45], while Petya attack encrypted entire hard drives rather than individual files, making systems completely unusable and was designed to destroy data[46]. The increase in cyber-attacks in recent years, the so-called '*cyberpandemic*'[47], in combination with the COVID-19 pandemic, which pushed many individuals and organizations to rely more on digital technologies for work, education, healthcare and social interaction, expanded the digital surface for cybercriminals.[48]

This shifted the focus to the protection of a wider range of digital infrastructure, taking into account the challenges posed by remote work, healthcare, and supply chain disruptions, while

[44] Vagelis Papakonstantinou, 'Cybersecurity as Praxis and as a State: The EU Law Path towards Acknowledgement of a New Right to Cybersecurity?' (2022) 44 Computer Law & Security Review 105653.

[45] 'The WannaCry Attack Reveals the Risks of a Computerised World' *The Economist* <https://www.economist.com/leaders/2017/05/20/the-wannacry-attack-reveals-the-risks-of-a-computerised world?utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=18151738051&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.directresponse.anonymous&gad_source=1&gclid=CjwKCAjwxNW2BhAkEiwA24Cm9Mi1uaLmGIUAgAZfsUaNfDc5JQG2XL0UPSt2zuA1BcI4GqVrMBxYhBoC5GIQAvD_BwE&gclsrc=aw.ds> accessed 2 September 2024.

[46] Alex Hern, 'WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017' *The Guardian* (30 December 2017) <https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware> accessed 2 September 2024.

[47] Grażyna Maria Szpor, 'The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland' (2021) 46 Review of European and Comparative Law 219.

[48] Rajesh Kumar and others, 'What Changed in the Cyber-Security after COVID-19?' (2022) 120 Computers & Security 102821.

remaining aware against traditional threats like malware and control system vulnerabilities.[49] In 2020, all of the above developments led to the European Commission introducing a proposal to amend the NIS Directive, which would be referred to as the NIS 2 Directive[50]. It was already evident from the Commission's draft that NIS 2 Directive seeked to expand upon the original Directive and address its limitations.[51] Notably, the draft NIS 2 Proposal adopted the Cybersecurity Act's definition of 'cybersecurity'. As a result, despite its technical focus, the NIS 2 Directive will not only aim to protect "network and information systems" but also "*the users of such systems and others impacted by cyber threats*"[52]. The scope of the NIS 2 Directive as defined in Article 1 reads as follows: "*this Directive sets out measures to ensure a high common level of cybersecurity within the Union",* thereby broadening its protective scope to include individuals as well, in contrast with its predecessor's scope, which was the functioning of the internal market.[53]

The NIS 2 Directive is considerably more comprehensive than its predecessor, with each chapter specifically designed to address the challenges posed by the original NIS Directive. For instance, Chapter I redefines the recipients of the Directive, categorizing them as 'essential' and 'important' entities to resolve issues caused by previous classifications. Chapter II outlines the requirements for Member States' national cybersecurity strategies, focusing on harmonization and greater consistency. Chapter III seeks to enhance cooperation and information sharing, while cybersecurity risk management and reporting obligations are thoroughly covered in the extensive Chapter IV, which is likely intended to be read in conjunction with Chapter V[54], which deals with information-sharing practices. Chapter VI, meanwhile, addresses supervision and enforcement but does not provide remedies to individuals. Rules deriving from NIS 2 Directive will be examined in the next chapter and always in regard to their link with privacy.

[49] 'Impact of COVID-19 on Cybersecurity' (Deloitte Switzerland) <https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html> accessed 2 September 2024.
[50] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L 333
[51] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM/2020/823).
[52] Papakonstantinou (n 44).
[53] See analysis above with regard to NIS Directive's subject matter and scope.
[54] Papakonstantinou (n 44).

CHAPTER A: PRIVACY AND GDPR COMPLIANCE AS A FOUNDATION FOR CYBERSECURITY

1. The Principles of Data processing under the GDPR and their Impact on Cybersecurity

1.1 The Concept of Personal Data

Over the years, personal data has become a critical component in the evolution of the digital age, with its collection, process and use contributing the most to online economy. Tech companies such as *Google* and *Meta* generate massive amount of revenue through the use of personal data, particularly with regard to targeted advertising. In fact, *Google* tracks about 40% of the world's web traffic, using it to tailor ads and content to individual users.[55] In addition, in Europe only 39% of online users read privacy policy statements before providing their personal data and an even lower number, around 36%, checked that the website where they provided their data was secure.[56] In general, companies gather data from various sources such as mobile apps, browsing habits, social media interactions, and smart devices to create analytical profiles of their users. This personal information, along with insights gained from user behavior, has turned into a valuable asset, as tech giants exploit this information, not only to deliver personalized content but also to conduct market research and enable precise advertising campaigns.[57] But the data is not always handled by reliable or secure entities and if exposed to unauthorized access, sensitive information and other personal data can be at risk. Having in mind the digital exploitation of data, the primary focus of the GDPR, which is to protect personal data and the fact that the GDPR applies only if the data being processed qualifies as personal data[58], it is time to examine what type of data are considered as 'personal data'.

Starting by the information that the GDPR itself provides in Article 4 '*personal data means any information relating to an identified or identifiable natural person',* while 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;'.* In practice, this encompasses all data that can be linked to a person in any way.[59] For example, personal data includes telephone numbers, credit card

[55] '41 Data Privacy Statistics and Facts You Shouldn't Ignore in 2024' (*PrivacySavvy*) <https://privacysavvy.com/security/safe-browsing/data-privacy-statistics/> accessed 4 September 2024.

[56] 'How Do EU Citizens Manage Their Personal Data Online?' <https://ec.europa.eu/eurostat/web/products-eurostat-news/-/edn-20220127-1> accessed 4 September 2024.

[57] Martina Lindorfer, The Threat of Surveillance and the Need for Privacy Protections (Introduction to Digital Humanism: A Textbook), 2024

[58] Article 29 Data Protection Working Party Opinion 04/2007 on the concept of personal data [2007] 01248/07/EN WP 136 and Article 2 of Regulation (EU) 2016/679.

[59] 'What Is Personal Data? - European Commission' <https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en> accessed 4 September 2024.

numbers, license plates, customer numbers and addresses. Additionally, given that the definition includes '*any information*'[60], the term '*personal data'* is interpreted as broadly as possible.

This approach was endorsed by case law of the Court of Justice of the European Union (hereinafter the 'CJEU') and can be manifested in its *Peter Nowak v Data Protection Commissioner* case[61], in which the CJEU considered less obvious information, such as written responses from a candidate during an exam, along with the examiner's comments, to be considered as personal data, in case the candidate can potentially be identified. In another notable case and more specifically in the *Patrick Breyer v Bundesrepublik Deutschland* case[62], the CJEU ruled that IP addresses can also fall under the category of personal data, if the data controller has the legal authority to require the internet service provider to supply further information to identify the individual associated with the IP address. Moreover, Article 4 of the GDPR specifies that personal data must refer to a natural person and therefore data protection rules do not possess any ground for application to information about legal persons, such as corporations, foundations, or institutions. For natural persons, however, protection begins with the acquisition of legal capacity, which starts at birth and ends at death, therefore, data must be linked to living and identifiable individuals to be considered personal data.

1.2 The Definition of Data Processing

Continuing with the necessary definitions and the meaning of '*data processing',* Article 4 of the GDPR provides for the relevant definition as well: '*processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'*. By this quite descriptive definition, it can be understood that the term 'data processing' is the process of data management. Considering that raw, unrefined data by itself holds little value for any organization, the procedure of data processing takes place with the ultimate goal of creating genuine and useful information from the data collected.[63] This process typically involves a series of steps carried out within an organization, in order to create more effective business strategies and gain a competitive advantage.[64]

[60] Regulation (EU) 2016/679 Article 4 para. 1.
[61] Judgment of the Court (Second Chamber) of 20 December 2017, Case C-434/16, *Peter Nowak v Data Protection Commissioner*, ECLI:EU:C:2017:994.
[62] Judgment of the Court (Second Chamber) of 19 October 2016, Case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:779.
[63] Paunović, Katarina. "Data Processing and Storage." Encyclopedia of Public Health, edited by Wilhelm Kirch, Springer Netherlands, 2008.
[64] 'What Is Data Processing: Cycle, Types, Methods, Steps and Examples | Simplilearn' (*Simplilearn.com*, 21 October 2020) <https://www.simplilearn.com/what-is-data-processing-article> accessed 7 September 2024.

It is clear from Article 4, that the notion of 'processing' is very broad, in line with the definition of personal data. It includes automated and non-automated means of processing as defined in Article 2, where the first involves utilizing software to handle data tasks autonomously, requiring little to no human input and the latter has the meaning of the processing that takes place exclusively when personal data is recorded and maintained solely in physical, paper format. A fine example of automated means of processing can be derived from the *František Ryneš* case[65], in which Mr. Ryneš used a domestic CCTV system to capture footage of two individuals vandalizing his property by breaking windows. The CJEU ruled that video surveillance involving the recording and storage of personal data qualifies as automated data processing, falling under the scope of EU data protection laws. The CJEU firstly concluded that an image captured by a camera system is considered personal data, as it is possible to identify a person, while regarding the part of the automated processing, the Court recognized that since the video recording was stored continuously and non-stop, it constitutes a form of automation in the collection, storage and recording of data.

1.3 Principles Governing the Processing of Personal Data

Now, that the main definitions were established, in this chapter, the primary focus will shift to the fundamental principles of data processing. Firstly, we will analyze their meaning, scope, and objectives, and then we will explore and evaluate their impact on helping organizations build strong cybersecurity foundations. One could say that, their significant place within the rules of the GDPR can also be endorsed by the fact that violations can lead to substantial administrative penalties. Article 83 of the GDPR sets out the general conditions for imposing administrative fines, in case of a breach of obligations with regard to the application of data processing principles. The administrative fines are imposed by the competent national supervisory authority and can result in fines of up to €20,000,000 or 4% of the company's total global annual revenue from the previous financial year; whichever amount is greater.[66] Considering the annual revenues of major corporations, it's reasonable to assume that these fines could reach very high figures.

Circling back to the data processing principles as enshrined in Article 5 of the GDPR, these include lawfulness, fairness, and transparency; purpose limitation; data minimization; data accuracy; storage limitation; integrity and confidentiality, and lastly accountability. Although all principles hold equal importance and ensure safe data processing, for the purposes of this thesis, we will focus solely on those that can be argued to have a direct contribution to the obligations arising from the NIS 2 Directive, limiting the effects of a cyber-attack and collectively contributing to the creation of a secure digital framework.

Starting off with the principle of integrity and confidentiality, also known as the data security principle, although not explicitly mentioned as such. The data security principle can be found in Article 5 para. 1 (f), which provides that '*personal data shall be processed in a manner*

[65] Judgment of the Court (Fourth Chamber), 11 December 2014, Case C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů,* ECLI:EU:C:2014:2428.
[66] Article 83 para. 5 of Regulation (EU) 2016/679.

that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'. In essence, data security mandates that suitable technical and organizational safeguards be put in place to protect personal data from unauthorized (accidental or not) or illegal access, use, alteration, disclosure, loss, destruction, or even damage.[67] In parallel with the wording of Article 32, both data controllers[68] and processors[69] have an obligation to take into account a number of factors, including the most recent technological advancements, the nature, scope and purpose of data processing, along with the potential risks to individuals' rights and freedoms when applying these safeguards. Another serious factor is the implementation costs of these measures, which will be evaluated in Part II of this thesis.

In practice, data security entails implementing strategies like pseudonymisation and encryption of personal data, as well as constantly caring out effectiveness and risk assessments, concerning the application of these safeguards, in order to maintain strong and effective data protection. More precisely, pseudonymisation is defined by the GDPR and is referenced many times as an appropriate safeguard. It can be understood as the processing of personal data, which takes place in a manner that the data can no longer be attributed to a specific data subject[70], without the use of additional information, which is kept separately and is subject to technical and organisational measures. Practically, pseudonymisation replaces identifying attributes ('identifiers') in personal data with a pseudonym and keeps those attributes separate.

In order to better understand how pseudonymisation works we will mention the simplest method of pseudonymisation, the so-called *counter method*, which replaces identifiers with numbers generated from a predefined number sequence.[71] Pseudonymisation does not only consist of the de-identification process, but also allows for re-identification of a data subject as well, in the processing stage. On the contrary, anonymised data, as a result of an anonymisation procedure do not fall under GDPR legal regime, pursuant to Recital 26 of the GDPR and while the definition of anonymisation is absent in the GDPR, Recital 26 clarifies that anonymous information, is information that does not relate to an identified or identifiable natural person[72], therefore not constituting personal data. In consideration of the above, the CJEU in *SRB v. EDPS* case[73] has ruled that pseudonymised data are still personal data and that the absence of supplementary

[67] European Union Agency for Fundamental Rights and Council of Europe (ed), *Handbook on European Data Protection Law* (2018 edition, Publications Office of the European Union 2018).

[68] According to Article 4 para. 7 data controllers are responsible for determining both the reasons for and the methods of processing personal data. In other words, they decide the means and reason behind a data processing activity. A data controller can be an individual or an organization, such as a company, small or medium-sized enterprise, or even a public authority, agency, or other entity.

[69] According to Article 4 para. 8 a "processor" refers to an individual or organization, including public authorities, agencies, or other entities, that processes personal data on behalf of the data controller.

[70] According to Article 4 para. 1, a data subject is an identified or identifiable natural person, which the personal data relates to.

[71] European Union Agency for Cybersecurity., *Data Pseudonymisation: Advanced Techniques and Use Cases : Technical Analysis of Cybersecurity Measures in Data Protection and Privacy*. (Publications Office 2021) <https://data.europa.eu/doi/10.2824/860099> accessed 8 September 2024.

[72] Felix Bieker and others (eds), *Privacy and Identity Management: 17th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Privacy and Identity 2022, Virtual Event, August 30–September 2, 2022, Proceedings*, vol 671 (Springer Nature Switzerland 2023) <https://link.springer.com/10.1007/978-3-031-31971-6> accessed 15 August 2024.

[73] Judgment of the General Court (Eighth Chamber, Extended Composition) of 26 April 2023, Case T-557/20, *Single Resolution Board v European Data Protection Supervisor*, ECLI:EU:T:2023:219.

information needed to identify individuals, does not automatically preclude the transmitted data from being considered as personal data.

On the other hand, data encryption is mentioned in parallel with pseudonymisation as an appropriate technical and organizational measure taken by organizations that act either as a data controller, or as a data processor.[74] In fact, encryption is considered a crucial tool for protecting sensitive information, such as personal, financial, and medical data, which are frequently targeted by cyberattacks. Encryption works in practice by firstly converting data into an encrypted form by the use of algorithms and then by creating decryption keys for each encrypted files, resulting in the authorization and access of parties that hold the right decryption information.[75] There are two primary methods of encryption, within the broader meaning of cryptography: symmetric encryption and asymmetric encryption. Symmetric encryption uses the same key for both encryption and decryption, making it proficient for encrypting large amounts of data in a small amount of time.[76] However, since all advantages are often accompanied by associated limitations, a major obstacle with symmetric encryption is the difficulty of securely transmitting the encryption key between the involved parties.[77] In contrast, asymmetric encryption utilizes a pair of keys: a public key for encryption and a private key for decryption, essential for processing.[78] While asymmetric encryption is slower than symmetric methods, it simplifies key distribution since only the private key must be kept secret. Additionally, an innovational approach in the field is homomorphic encryption. Homomorphic encryption allows for the processing of data while being encrypted. This approach maximizes data privacy by allowing computations to be carried out directly on encrypted files, while enhancing data confidentiality and substantially reducing the burden of repetitive encryption and decryption processes.[79] This makes it an appealing choice for organizations that use cloud computing and data analytics.

Pseudonymisation and encryption of data are privacy-preserving techniques[80] that also allow for the identification of data subjects when necessary. Their effectiveness must be regularly reviewed and updated as needed, and the cost of implementation should be balanced against the potential risks. In the event of a security incident that affect the confidentiality and integrity of personal data, or in simpler words in the event of a data breach due to unauthorized access, pseudonymisation and encryption play a key role in aligning data protection principles with appropriate technical safeguards. Pseudonymization is also a critical component of privacy by design[81], which integrates data protection into the core of data processing systems.

The second principle, which will be analysed for the purpose of this thesis, is the data minimization principle, as enshrined in Article 5 para. 1 (c) of the GDPR. In GDPR's own words

---

[74] Article 32 para. 1 (a) Regulation (EU) 2016/679.
[75] Srinivasan Nagaraj, GSVP Raju and V Srinadth, 'Data Encryption and Authetication Using Public Key Approach' (2015) 48 Procedia Computer Science 126.
[76] Yuanjian Li and others, 'An Efficient Encryption Method for Smart Grid Data Based on Improved CBC Mode' (2023) 35 Journal of King Saud University - Computer and Information Sciences 101744.
[77] Ibid.
[78] Javier Guerrero and others, 'Encryption Techniques: A Theoretical Overview and Future Proposals' (2016).
[79]'Craig Stuntz - What Is Homomorphic Encryption, and Why Should I Care?' <https://www.craigstuntz.com/posts/2010-03-18-what-is-homomorphic-encryption.html> accessed 25 August 2024.
[80] Damian Eke and Bernd Stahl, 'Ethics in the Governance of Data and Digital Technology: An Analysis of European Data Regulations and Policies' (2024) 3 Digital Society 11.
[81] Article 25 of Regulation (EU) 2016/679.

'*personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*'.[82] In essence, the data minimization principle requires data controllers to ensure that personal data is '*adequate, relevant, and limited to what is necessary*' for the specific purposes for which it is processed. Practically, the GDPR permits personal data processing only when the processing meets three conditions: it is adequate, meaning it is sufficient for achieving the intended purpose; it is relevant, meaning it is directly related to that purpose, and includes only the amount of information necessary.[83] Additionally, data processing should occur only when the purpose cannot reasonably be fulfilled by other means.[84] Compliance with these requirements of course must be assessed on every respective processing procedure, after taking into account each individual or group affected by the processing, and should be reviewed regularly.

Adhering to the principle of data minimization offers businesses benefits that can also help mitigate the risk of online threats. By collecting and processing only the data necessary for specific purposes, the risk of data loss and most specifically the risk of data breaches is significantly reduced. Efficient data storage also allows for quicker responses to data access requests from individuals, which enhances the organization's trustworthiness and customer satisfaction. Moreover, retaining excessive data is not only potentially unlawful but also can result in serious and costly situations, in case of a breach.

The principle of data minimization operates on two levels, with regard to time and volume. The first level addresses the volume and amount of data that are collected and eventually stored, while the second aspect concerns the length of time the data is kept. Because of this, data minimization is closely linked to the principle of storage limitation, which mandates that data be retained only as long as necessary, with retention periods kept to a strict minimum[85].

The importance of data minimization has been affirmed by the CJEU in its *Digital Rights Ireland and Seitlinger and others v Minister for Communications* case, although not specifically mentioning the principle of data minimization, it used its logic behind it for its ruling.[86] In particular, although the focus of the ruling was on the compatibility of the Data Retention Directive (2006/24/EC) with fundamental rights of respect for private and family life and of protection of personal data under the Charter. In detail, the Data Retention Directive was an EU directive, which required telecommunications and internet service providers to gather certain data about their users for law enforcement purposes, with a view to assisting in the investigation and prosecution of serious crime, with a special focus to terrorism and organized crime. The Directive obliged providers to collect metadata of communications for a period up to 2 years, therefore there was much criticism on the basis of mass surveillance and the following infringement of the aforementioned fundamental rights.

The Court ruled that the Data Retention Directive imposed obligations on telecommunications and internet service providers to collect and store disproportionate amounts

[82] Article 5 para. 1 (c) of Regulation (EU) 2016/679.
[83] Angeliki Barmpetaki, "Data protection: A still developing area in the EU legal order" (LL.M thesis, National and Kapodistrian University of Athens 2023).
[84] Recital 39 of Regulation (EU) 2016/679.
[85] Ibid.
[86] Judgment of the Court (Grand Chamber), 8 April 2014, Joined Cases C-293/12 and C-594/12., Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, ECLI:EU:C:2014:238.

of personal data, without any sufficient safeguards for privacy and data protection. The Court determined that the collection and storage of large amounts of users' personal data was excessive and unnecessary, resulting in the violation of the principles of proportionality and necessity in data processing.[87] That is particularly interesting given that there is a close relation between the principle of data minimization under the GDPR and the principle of proportionality. It can be argued that proportionality is actually enshrined in the data minimization principle, due to fact that it mandates only the collection of data that is strictly necessary for the processing.

Therefore, while the principle of data minimization is not explicitly mentioned in *Digital Rights Ireland* case, the judgment indirectly endorses it by highlighting the need for data processing to be limited to what is strictly necessary, ensuring that personal data collection is both relevant and proportionate to the purpose at hand.

2. Privacy by Design and the Integration of Data Protection Principles into System Development

Pseudonymisation and encryption of data are privacy-preserving techniques[88] that also allow for the identification of data subjects when necessary. Their effectiveness must be regularly reviewed and updated as needed, and the cost of implementation should be balanced against the potential risks. In the event of a security incident that affect the confidentiality and integrity of personal data, or in simpler words in the event of a data breach due to unauthorized access, pseudonymisation and encryption play a key role in aligning data protection principles with appropriate technical safeguards. In the general context of privacy-preserving and privacy-enhancing technologies ('PETs'), PETs are tools and methods developed to safeguard sensitive data, while preserving the confidentiality and integrity of information.[89] They serve as protective measures, ensuring that personal data stays secure, even during data collaboration and analysis.

There have been several definitions for PETs from different actors over the years, including the Organisation for Economic Cooperation and Development's ('OECD') definition that provides that '*Privacy-enhancing technologies (PETs) commonly refer to a wide range of technologies that help protect personal privacy. Ranging from tools that provide anonymity to those that allow a user to choose if, when and under what circumstances personal information is disclosed, the use of privacy-enhancing technologies helps users make informed choices about privacy protection'*[90], as well as the definition provided by the European Union Agency for Cybersecurity ('ENISA'), which refers to PETs as '*software and hardware solutions, such as systems encompassing technical processes, methods, or knowledge to achieve specific privacy or data protection functionality or to protect against risks to privacy of an individual or a group of*

[87] Ibid.
[88] Eke and Stahl (n 80).
[89] Ira S Rubinstein, 'Regulating Privacy By Design', 2011.
[90] Organisation for Economic Co-operation and Development, 'Inventory of Privacy-Enhancing Technologies (PETs)', 2002.

natural persons'[91]. It can be understood that even though all definitions include different elements, they all have the same meaning; the methods and tools used that enhance privacy.

In addition, the list and use of privacy-enhancing technologies can be further developed through advanced machine-learning models[92]. Nonetheless, these models are often carried outside of Europe, usually in cloud systems in the United States[93] and therefore the legal requirements for the transfer of data must be guaranteed. A very important judgment of the CJEU with regard to legal transfer of data could provide some legal ground for these requirements to be met, in addition with the Articles of the GDPR concerning transferring of data. In *Schrems II* case the CJEU invalidated the EU-U.S. Privacy Shield for data transfers due to concerns over U.S. surveillance practices, after Facebook Ireland used Standard Contractual Clauses ('SCCs') for transferring personal data to its U.S. parent company.[94] The Court emphasized that transfers under SCCS can take place when appropriate safeguards are put in place and only when it can be guaranteed that the third-country, to which the data will be transferred, has an equivalent level of protection of personal data similar to the one offered in the EU by the GDPR. One could argue that these appropriate safeguards could be achieved through the application of privacy-enhancing technologies. This way organizations that process data for online marketing through data analytics can gain valuable insights from datasets while ensuring that the privacy of individuals whose information is included remains protected.[95]

Privacy-enhancing technologies are a critical component for the implementation of privacy by design[96], which integrates data protection into the core of data processing systems. The GDPR and especially Article 25, where privacy by design is established, mandates that the above measures of technical nature be implemented in a way so as to integrate the appropriate safeguards into the processing of data but also before this stage, in the determination of the means for processing. What Article 25 mandates in essence is an *a priori* consideration of how to properly and effectively integrate data protection principles into the designing and construction of information and communication technology systems ('ICT systems') including hardware, software, networks and data storage, in order to enhance privacy. Privacy must be a fundamental element of every standard process and planning operation of any organization based on a proactive, rather than reactive approach, which allows for predicting the occurrence of events that invade privacy.[97]

Privacy by design aims to provide the highest level of privacy by ensuring that personal data is safeguarded automatically in any IT system and is integrated into systems before the data is collected, ensuring that security is maintained throughout the entire data lifecycle, as robust security measures are crucial from the moment data is acquired until it is properly disposed of at

[91] European Agency for Cybersecurity, Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies, 2016.
[92] Bieker and others (n 72).
[93] Ibid.
[94] Judgment of the Court (Grand Chamber) of 16 July 2020, Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559
[95] 'Data Protection by Design and Default' (1 July 2023) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and governance/data-protection-by-design-and-default/> accessed 12 September 2024.
[96] Article 25 of Regulation (EU) 2016/679.
[97] Ann Cavoukian, 'Privacy by Design The 7 Foundational Principles', Implementation and Mapping of Fair Information Practices.

the end of its use.[98] This guarantees that data is securely handled at every stage, from beginning to end. Privacy by design upholds comprehensive protection and management of information throughout its entire existence, ensuring continuous safeguarding without any breaks in security or accountability. The application of the principle of security as explained above is particularly important, as privacy cannot exist without strong, reliable security.

Some key privacy by design tools include and are not limited to anonymizing, pseudonymizing or encrypting personal data the moment the data is entered into the IT system, limiting the data collected automatically by apps to only what is absolutely necessary, integrating privacy notifications into systems in a user-friendly manner that are easy to understand, implementing time limits on data retention and offering straightforward and accessible privacy settings.[99] All of these strategies are placed under the umbrella of encouraging system designers and engineers to consider privacy concerns during the development of IT systems as a general 'rule'.[100] Nonetheless, one could think that such encouragement cannot take place without extensive training on privacy requirements under the current legislative framework on behalf of developers.[101]

Additionally, for the purposes of this Chapter, it is crucial to make a distinction between tools that developers can rely on in enhancing privacy, such as the so-called front-end software development and back-end data management. Front-end activities focus on the creation and design of customer-oriented products and services, which includes software that customers can download, the web services they use, as well as the personal information they share or content they generate.[102] In contrast, back-end practices involve the management of data to ensure that information systems used internally or even shared with third partners, comply with privacy regulations, internal company policies and individual customer privacy preferences.[103] Overall, the general data management strategy emphasizes on how companies should design and manage their information systems with privacy as a priority, guiding employees in accessing, using and disclosing data.

While these two domains are unique, they do overlap to some extent, as most internet-based products and services combine elements of both front-end design and back-end data handling. The software development lifecycle aims to ensure that developers take into account customer privacy expectations along with relevant security threats, when creating products and services, resulting in empowering individuals (and most importantly users) by improving their awareness of what personal information will be collected, how it will be utilized and the options available to them regarding the management of their data, including transfer, storage, and usage.

---

[98] Ibid.

[99] Lilian Edwards, 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective' [2016] SSRN Electronic Journal <http://www.ssrn.com/abstract=2711290> accessed 25 August 2024.

[100] Ewa Luger, Lachlan Urquhart, Tom Rodden and M. Golembewski "Playing the Legal Card: Using Ideation Cards to Raise Data Protection Issues within the Design Process" Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 15), Seoul, 18-23 April 2014.

[101] Edwards (n 93).

[102] 'What Is Front End Development? Comprehensive Guide | Multishoring' (16 April 2024) <https://multishoring.com/blog/what-is-front-end-development/> accessed 13 September 2024.

[103] 'Back End : A Complete Overview on Its Relevance in Data Science' <https://datascientest.com/en/all-about-back-end> accessed 13 September 2024.

It is, also, widely known that many multinational IT companies have already created internal frameworks, policies and systems aimed at incorporating privacy into their software development and data management practices. A notable example is Microsoft's Security Development Lifecycle ('SDL'), which exemplifies how to be mindful of privacy considerations into the design process. The SDL is designed to embed privacy and security principles throughout the five phases of the software development lifecycle, including stages of requirements gathering, design, implementation, verification, and release.[104] On the other hand and with regard to data management, IBM's Tivoli Privacy Manager serves as an extensive privacy management solution for organizations that offers a range of privacy-related functions.[105]

This approach to privacy aims to mitigate the likelihood of privacy breaches, such as unexpected data collection or unauthorized use and exposure, while building digital security. Privacy considerations significantly influence and enhance digital security by emphasizing the protection of personal data.[106] While these considerations focus on safeguarding privacy rights, they also stress the need for security measures to protect sensitive information, under the general framework of digital security, which will be analysed thoroughly in the next Chapter.

CHAPTER B: THE REINFORCEMENT OF CYBERSECURITY IN DATA PROTECTION OBLIGATIONS

1. The Concept of Cybersecurity and its Significance in Safeguarding Personal Data

Since the introduction of the EU Cybersecurity Strategy by the Commission in 2013 as explained before, Europe's legal landscape for cybersecurity has undergone major transformations in the years to come. The most significant milestones in this transformation include the enforcement of the NIS Directive, which led to important national legislation in Member States between 2016 and 2018, ultimately resulting in the repealing of NIS Directive and the adoption of NIS 2 Directive in 2022. Since its implementation, NIS 2 Directive has placed cybersecurity as a central focus in the management of critical infrastructures through technological and

[104] 'Microsoft Security Development Lifecycle' <https://www.microsoft.com/en-us/securityengineering/sdl> accessed 14 September 2024.
[105] 'Tivoli Federated Identity Manager 6.2.2.6' (7 March 2021) <https://www.ibm.com/docs/en/tfim/6.2.2.6?topic=management-policy-tivoli-security-policy-manager> accessed 14 September 2024.
[106] Petar Radanliev, 'Digital Security by Design' [2024] Security Journal <https://link.springer.com/10.1057/s41284-024-00435-3> accessed 15 August 2024.

organizational measures. The focus of NIS 2 Directive is shifted towards a more comprehensive, risk-based, and situational awareness-driven approach to cybersecurity.[107]

Similar to the GDPR's data breach notification obligations, NIS 2 Directive requires the reporting of significant cyber incidents to the competent national authority[108]. Naturally, this reporting requirement demands strong situational awareness along with strong monitoring and analysis within organizations. While the obligation to report major cyber incidents is among the most immediate and widely discussed effects, the broader goal, as outlined in Article 1, is to achieve a high and uniform level of network and information system security across the EU. Both the GDPR and NIS 2 Directive impose data breach and incident reporting requirements that necessitate the entities' ability to detect and assess the impact of incidents. To meet these obligations, organizations must develop strong security capabilities, enabling them to effectively monitor and respond to potential threats, as explained in this Chapter.

Within the framework of digital security and cybersecurity, with these terms used interchangeably, digital security encompasses a wide range of strategies and techniques, each addressing different vulnerabilities, aimed at safeguarding networks and data from cyberattacks, unauthorized access, or damage[109], resulting in a secure environment for communications, data processing, use and storage, and most importantly transactions. For the sake of this thesis, when referring to the term cybersecurity, it will have the meaning given by Myriam Dunn Cavelty. She notes that '*cyber-security is a type of security that unfolds in and through cyberspace; the making and practice of cyber-security is both constrained and enabled by this environment'*[110]. It can be already understood that the cybersecurity is closely connected to cyberspace and cannot exist outside of it. When referring to cyberspace on the other hand, it can be primarily understood as a digital environment, in which online communication takes place. Cyberspace allows users to exchange information and interact with each other, share ideas, participate in social fora, make transactions and even create innovative media, among numerous other activities.[111] But it is in fact more than that. Cyberspace represents a social concept, as it is socially shaped by the billions of individuals who engage with it and are interconnected within its vast network.[112] Essentially, '*cyberspace is what human societies make of it'*[113]. This anthropocentric approach to cyberspace allows for the transformation of the digital environment from a mere collection of data and information into an interactive space that fosters human connection and collaboration[114], which emphasizes the need for the protection of individuals' fundamental rights.

---

[107] Dietmar PF Möller, *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices*, vol 103 (Springer Nature Switzerland 2023) <https://link.springer.com/10.1007/978-3-031-26845-8> accessed 15 August 2024.

[108] Article 23 of Directive (EU) 2022/2555.

[109] Ibid.

[110] Myriam Dunn Cavelty, 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse' (2013) 15 International Studies Review 105, p. 107.

[111] 'Cyberspace' (*Techopedia*, 26 June 2023) <https://www.techopedia.com/definition/2493/cyberspace> accessed 18 September 2024.

[112] Denise M Carter, 'Cyberspace and Cyberculture' in Audrey Kobayashi (ed), *International Encyclopedia of Human Geography (Second Edition)* (Elsevier 2020) <https://www.sciencedirect.com/science/article/pii/B9780081022955108108> accessed 18 September 2024.

[113] 'Cyberspace' (n 105).

[114] Julio Navío-Marco, 'Cyberspace as a System and a Social Environment: A Theoretical Proposal Based on Niklas Luhmann'.

One of the strategies that derive from the notion of cybersecurity is network security, which is designed to protect networks from unauthorized access, guaranteeing their continued functionality and the integrity and security of the data they handle. Network and information security is the primary objective of NIS 2 Directive,[115] and its Recital can provide a better understanding of its objectives, scope, and application; therefore, the examination will begin there.

Starting with the entities that have cybersecurity risk-management measures and reporting obligations within the framework of NIS 2 Directive, Member States have the responsibility of establishing a list of essential and important entities that fall under the regime of NIS 2 Directive.[116] In this regard and with a goal to creating uniform application among Member States, a 'safety net' was established, which implemented a uniform criterion based on the size of the entity pursuant to Article 2 of the Annex to Commission Recommendation 2003/361/EC[117], whereby all medium-sized enterprises, or those exceeding this threshold and operating in the specified sectors, fall within its scope.

Essential and important entities, except for medium-sized ones, are mentioned in Article 3 of NIS 2 Directive. These include trust service providers and top-level domain registries, providers of public electronic communications, public administration entities, entities identified as critical under Directive (EU) 2022/2557[118] and any other entities listed in Annex I or II of NIS 2 that are identified by a Member State as essential entities. Annex I covers entities in sectors such as energy, health, banking, financial markets, and notably, digital infrastructure, which includes internet exchange point providers[119], DNS service providers[120], TLD name registries[121], cloud computing service providers, data center service providers, and providers of public electronic communications networks. Annex II includes digital service providers, such as online marketplaces, search engine providers, and social networking platforms. Digital infrastructure providers have also a parallel obligation to the adoption of cybersecurity risk-management measures, which is related to the physical security of the entity, given the close relation of cybersecurity and physical security.[122]

With regard to the cybersecurity risk-management measures that essential and important entities under NIS 2 must implement, Article 21 of NIS 2 Directive mandates that technical and organizational practices must be taken, in order to foresee and address the risks related to the entities' security systems, used for their services and to reduce the impact of incidents, in case they do happen. The above measures are explained in the second paragraph of Article 21, which states

[115] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L 333.
[116] Recital 7 of Directive (EU) 2022/2555.
[117] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, OJ L 124, 20.5.2003.
[118] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, OJ L 333, 27.12.2022.
[119] Internet service providers and other internet infrastructure companies use physical locations through which they connect, known as internet exchange point providers.
[120] The Domain Name System (DNS) converts domain names into IP addresses, enabling browsers to access websites and other online resources.
[121] A Top-Level Domain (TLD) is the final part of a domain name, appearing after the last dot, and is used to indicate a website's category or country code.
[122] Recital 30 and 31 of Directive (EU) 2022/2555.

that the entities' focus must be shifted towards an all-hazards strategy designed to establish the security of their systems, along with their physical infrastructure against any potential incidents.

These measures should encompass, at a minimum, the following elements: strategies for conducting risk assessments concerning the security of information systems; procedures for managing and responding to incidents, including disaster discovery protocols; safeguarding the supply chain between entities and their direct suppliers or service providers; security measures related to the development and maintenance of network and information systems, as well as the adoption of multi-factor authentication methods within the organization and appropriate training for employees and staff, with regard to access control and the management of systems.

Additionally, Article 21 entails the adoption of proper and thorough guidelines and processes for, on the one hand, evaluating the effectiveness of cybersecurity risk management practices and, on the other, implementing cryptographic solutions and encryption protocols. Lastly, Article 21 mentions the need for the adoption of fundamental cyber hygiene practices, for which a separate analysis must be made, due to the ambiguity of this term. On a last note, it has to be mentioned that Member States have a supervisory role in the implementation of these safeguards by essential and important entities.

As shown in Article 21, for the purpose of effectively safeguarding an organization from cyberthreats, implementing a range of security measures is essential to achieve a robust level of cybersecurity. In order to specify which exactly is the nature of these technical initiatives, a few examples will be provided. First off, it is essential to establish a network perimeter defense, which acts as the initial barrier against threats. In essence, a perimeter defense, is a protective system surrounding the network, aimed at preventing external threats from gaining access.[123] A firewall is the primary tool for this, as it creates a division between the internal, trusted network and the external, untrusted one. What it does is that, it manages and filters traffic between these two zones, the internal and external one, enforcing the organization's security policies by either allowing or blocking communication based on predefined rules.[124]

When external users need remote access, a Virtual Private Network ('VPN') is typically used. In this case, users connect to the firewall and authenticate their identity, after which a secure, encrypted connection—known as a VPN—is established between their device and the organization's internal network.[125] This ensures that only verified users can have access to the internal system of an organization. Additional layers of protection are, also, provided by endpoint security software, which includes tools such as antivirus programs and access control features, such as data encryption.[126] This type of softwares can also regulate which devices, like USB storage, are permitted to connect to the network, enhancing the overall security posture of an organization.

[123] Izzat Alsmadi, *The NICE Cyber Security Framework: Cyber Security Intelligence and Analytics* (Springer International Publishing 2023) <https://link.springer.com/10.1007/978-3-031-21651-0> accessed 21 September 2024.
[124] Ibid.
[125] Valentin Mulder and others (eds), Trends in Data Protection and Encryption Technologies (Springer Nature Switzerland 2023).
[126] Sofia Terzi and Ioannis Stamelos, 'Architectural Solutions for Improving Transparency, Data Quality, and Security in eHealth Systems by Designing and Adding Blockchain Modules, While Maintaining Interoperability: The eHDSI Network Case' (2024) 14 Health and Technology 451.

Application security is another element of cybersecurity, which focuses on securing software and devices from malicious actors by identifying and addressing vulnerabilities in software applications throughout their entire lifecycle and more specifically from development to deployment.[127] A breach in application security can allow attackers to access sensitive data that the software is meant to protect. In addition to application security, operational security plays a vital role. It involves policies and processes that dictate how data should be stored, transferred, and accessed.[128] This includes managing user access to corporate networks and ensuring the proper protection of data assets.

Nonetheless, simply installing security mechanisms is not sufficient enough on its own for achieving a high level of cybersecurity, particularly as an organization grows in size and complexity.[129] Effective risk management within an organizations, which involves identifying, evaluating, and mitigating potential threats, plays a key role in enhancing cybersecurity. This process starts by identifying the most critical system assets, assessing the threats they face, and implementing appropriate controls to minimize the potential impact of any incidents. This resembles to the proactive approach that privacy by design mandates as well, as analysed in Chapter A.[130] Moreover, organizational security measures are guided by the ISO 27000 family of standards[131], which focus on the protection of an organization's information systems.[132] Adhering to these standards demonstrates that an organization has implemented proper compliance procedures for managing information security in line with industry best practices, as defined in Article 25 of NIS 2 Directive.

As discussed in the previous section, essential and important entities have obligations to protect personal data, pursuant to various technical and organizational mechanisms available to achieve this. However, many existing cybersecurity measures do not have a comprehensive approach, particularly when it comes to safeguarding data used during daily operations.[133] Current cybersecurity practices may not fully address these complexities. To resolve this deficiency, a new framework for managing cybersecurity knowledge is necessary, one that fosters a holistic understanding of an organization's cybersecurity landscape at every level.[134] To achieve this, two key elements must be prioritized: The first one is collaboration across the organization. Cybersecurity must be viewed as a collective responsibility, within every department and employee, not just the IT team. This requires fostering an awareness culture, as well as

[127] 'What Is Application Security?, IBM' (5 June 2024) <https://www.ibm.com/topics/application-security> accessed 21 September 2024.
[128] 'Operational Security - an Overview, ScienceDirect Topics' <https://www.sciencedirect.com/topics/computer-science/operational-security> accessed 21 September 2024.
[129] Jerry Andriessen and others (eds), Cybersecurity Awareness, vol 88 (Springer International Publishing 2022).
[130] Ann Cavoukian, 'Privacy by Design The 7 Foundational Principles', Implementation and Mapping of Fair Information Practices.
[131] ISO/IEC 27000 family is the most widely recognized global standard for information security management systems (ISMS) and their associated requirements. These standards provide organizations, regardless of size or industry, with the tools to effectively safeguard assets, including financial data, employee records and third-party entrusted information.
[132] 'ISO - ISO/IEC 27000 Family — Information Security Management' (ISO, 25 October 2022) <https://www.iso.org/standard/iso-iec-27000-family> accessed 21 September 2024.
[133] Andriessen and others (n 123).
[134] Möller (n 101).

proactiveness and providing specific cybersecurity training that reflects how threats impact specific departments and what can employees do to avoid them.[135]

Additionally, effective collaboration and communication between organizations established in the same Member State and external expert groups, like the CSIRTs[136], is crucial for staying informed and prepared. Collaborative approaches on security shared by cybersecurity communities can help organizations gain a clearer understanding of the evolving cybersecurity landscape. The second element that contributes to the adopting a holistic approach to cybersecurity is real-time monitoring and proactively acting: The approach to achieving this by an organization is by continuously monitoring and evaluating the security of critical assets in real time and detecting cybersecurity threats and attacks as they happen, through data-driven risk and incident management that foster situational awareness.[137] The use of artificial intelligence ('AI') can also help identify abnormal behavior in large datasets as a method that supports proactive threat detection and response.[138]

Apart from the positive action, cybersecurity, also, extends to business continuity and disaster recovery planning. This comes at a later stage and only if a security breach has taken place. It involves the preparation of strategies to restore normal operation after a security breach, including ensuring that data remains safe, available, and private.[139] Another aspect of this incident recovery planning is system self-healing, which can be understood as the automated prevention or mitigation of cyber incidents, which can be fulfilled through applying patches to vulnerable software when monitoring detects an issue.[140] For this to function effectively, an organization must have a deep understanding of its own systems and dependencies, enabling it to understand where configuration changes could prevent or neutralize specific cyber threats.

Furthermore, access to current threat intelligence is crucial, as it provides details with regard to attacks and outlines potential mitigation strategies, which then allows AI-infused systems to generate appropriate responses tailored to each system and its needs[141]. These requirements are supported by the collaborative cybersecurity awareness model as described earlier, which leverages threat intelligence from cybersecurity communities. For example, both NIS 2 Directive (Article 23) and the GDPR (Article 33) mandate the sharing of certain cyber incident information under specific conditions. The difficulty is in identifying all relevant data that accurately describes an incident. A well-designed awareness system, based in a basic understanding of system architecture and interdependencies, can automatically identify key information sources and extract the necessary data. This data can then be shared with cybersecurity communities or authorities, optimizing the procedure for gathering and submitting incident reports.[142] Therefore, taking into account every presented in this paragraph, in order to achieve compliance with NIS 2 Directive,

[135] Gregory J. Touhill & Touhill, C. Joseph (2014), Cybersecurity for executives: A practical guide, John Wiley & Sons.
[136] Computer security incident response teams (CSIRTs). See footnote no. 37.
[137] Andriessen and others (n 123).
[138] Masike Malatji and Alaa Tolah, 'Artificial Intelligence (AI) Cybersecurity Dimensions: A Comprehensive Framework for Understanding Adversarial and Offensive AI' [2024] AI and Ethics.
[139] Andriessen and others (n 123).
[140] KA Taipale, 'Cyber-Deterrence' (1 January 2009) <https://papers.ssrn.com/abstract=1336045> accessed 21 September 2024.
[141] Malatji and Tolah (n 132).
[142] Andriessen and others (n 123).

both technical and organizational measures must be implemented. Organizations by being compliant with the above obligations not only ensure data privacy but also enhance the organization's overall security and elevate cybersecurity standards across the EU.

2. Conceptualizing Cyber Hygiene and Cyber Resilience

Continuing with the Recital of NIS 2 Directive, as it gives a first insight into the reasoning for the adoption of cybersecurity measures and a more detailed analysis of the legal obligations imposed, it states that when it comes to cyber hygiene policies, these provide the grounds for the protection of network and information system infrastructures, software and online application security.[143] Recital 49 continues by establishing that cyber hygiene policies consist of a collection of measures, with the meaning of frequent software and hardware updates, mandatory password changes and data back-ups, which create a proactive framework for the safety and security of digital infrastructure. Cybersecurity awareness could, also, help with building a strong level of security within the EU, through a common understanding of the risks the Union faces in the field of its cyberspace.[144]

Nonetheless, a common and uniform approach with regard to the definition of cyber hygiene, would be hard to find. Usually, it can be found through multiple IT advice on how to adopt the most effective defense techniques through anti-virus softwares or other suggestions on effectively safeguarding hardware.[145] This lack of clarity and vague definition around such a critical concept, in addition to the broad interpretation and minimal real-world testing, has not proved itself of use in building cyber resilience. Instead, it only creates confusion for IT managers and digital users, by sometimes offering contradictory guidance.[146] To truly achieve cyber resilience through cyber hygiene practices, it is important to clearly define cyber hygiene, explain its importance and establish its boundaries. Therefore, only through these considerations, the current cyber hygiene levels can be assessed, by identifying gaps and finding effective solutions to address those shortcomings.

The concept of cyber hygiene is borrowed from the idea of personal hygiene in public health sector. In a comprehensive report on cyber hygiene practices worldwide, the European Union Agency for Network and Information Security explained that '*cyber hygiene should be treated like personal hygiene. Once fully incorporated into an organization, it becomes a set of simple daily routines, healthy practices, and periodic checkups to ensure the organization's online well-being is optimal*'[147]. Having in mind that the term 'hygiene' typically serves as a set of guidelines, emphasizing what actions individuals should take and remain conscious of, cyber hygiene can be

[143] Recital 49 of Directive (EU) 2022/2555.
[144] Ibid Recital 50.
[145] Arun Vishwanath and others, 'Cyber Hygiene: The Concept, Its Measure, and Its Initial Tests' (2020) 128 Decision Support Systems 113160.
[146] Ibid.
[147] European Union Agency for Network and Information Security, Review of Cyber Hygiene Practices. (Publications Office 2016) <https://data.europa.eu/doi/10.2824/352617> accessed 20 September 2024.

understood as the cybersecurity practices that individuals need to follow to protect their personal information on internet-connected devices in order to be protected from cyber-threats and cyber-attacks.[148] In addition, the report made by ENISA also confirmed the lack of agreement on what cyber hygiene actually entails.

Different countries, including each of the Member States, have their own guidelines and recommendations, but there is no universally accepted standard or unified framework for organizations to assess and measure their cyber hygiene practices. If a standard approach was to be adopted and then further modified and customized by each Member State, the key areas would include measures, such as safeguarding networks and individual devices and ensuring secure cloud usage and supply chains.[149] More specifically, the above would be practically implemented through actionable steps, in the form of keeping a detailed record of all software to ensure timely patching, following secure configuration and hardening guidelines for devices, control and monitoring data entering, regularly backing up data and testing recovery processes and most importantly developing and implementing an incident response plan.[150]

In conjunction with the above, we understand that cyber hygiene has a more of a 'nice to have' approach towards cybersecurity, as it includes guidelines that beneficial in the general framework of security. Cyber hygiene rules can also help to building cyber resilience. Concerning the term cyber resilience the same ambiguity exists as with the term cyber hygiene. The term cyber resilience is a relatively new concept, gaining recognition in the early 2000s, as a method to address the growing need for systems capable of withstanding and recovering from cyber incidents.[151] Since then, it has grown to be of significant importance to organizations, due to the fact that they have become increasingly dependent on technology and are facing numerous cyber threats as a result. After the technological innovations that took place in these past 20 years, cyber resilience is seen as a crucial component of any robust cybersecurity strategy, enabling businesses to minimize the effects of attacks and ensure business continuity.[152]

The term 'resilience' can be understood as the ability of a material to absorb energy during elastic deformation and release it upon returning to its original shape.[153] More broadly and in the context of this thesis, resilience can be also understood as a system's capacity to absorb disruptions before undergoing structural changes, as all systems, to some degree, are vulnerable to failure.[154] Resilience involves anticipating and specifically adapting to these challenges when they happen, showcasing flexibility and responsiveness. If we had to choose one word to represent its core meaning, 'adaptability' would be the most fitting. This is because it highlights an organization's or system's capacity to adjust to shifting conditions and recover from cyberattacks. The notion of cyber resilience goes beyond just preventing threats. It also entails recovering plans, learning and

[148] Vishwanath and others (n 139).
[149] European Union Agency for Network and Information Security (n 121).
[150] SentinelOne, 'Cyber Hygiene: 10 Basic Tips For Risk Mitigation' (*SentinelOne*, 4 December 2018) <https://www.sentinelone.com/blog/practice-these-10-basic-cyber-hygiene-tips-for-risk-mitigation/> accessed 20 September 2024.
[151] Vasiliki Tzavara and Savvas Vassiliadis, 'Tracing the Evolution of Cyber Resilience: A Historical and Conceptual Review' (2024) 23 International Journal of Information Security 1695.
[152] Ibid.
[153] Gunderson, L., Holling, C.: Panarchy: Understanding Transformations in Human and Natural Systems. Bibliovault OAI Repository, p. 114. The University of Chicago Press (2003)
[154] Tzavara and Vassiliadis (n 145).

evolving in response to them. Lastly, research on the development of cyber resilience shows that organizations which prioritize it and take a proactive stance on cybersecurity are better positioned and can overcome them more easily and less costly.

Interim conclusion

Even though it may not be apparent at a first glance, the GDPR and especially its principles for lawful processing of data provide an enormous ground for application of technical safeguards that after being implemented, enhance privacy and security. Moreover, it is very interesting to consider how the abundance of technological innovations, such as encryption, were developed in order to protect personal data and sensitive information, affirming the primacy of legislation in guiding actions, decisions and even innovations.

By adhering to the GDPR's data processing principles and implementing privacy by design, organizations can create a strong foundation for cybersecurity and data protection. This not only helps protect personal data from unauthorized access and breaches but also builds trust among individuals, users and society. Integrating privacy considerations into system development ensures that data is handled securely throughout its lifecycle, ultimately contributing to a more secure and privacy-enhancing digital landscape.

The NIS 2 Directive, on the other hand, mandates a comprehensive approach to cybersecurity, encompassing technical measures, practices and employee training within an organization. When prioritizing legal compliance and implementation of the above analysed technical measures, organizations can achieve a strong level of cybersecurity, allowing for both data privacy and overall security of digital networks and physical system infrastructure.

The concepts of cyber hygiene and cyber resilience, while lacking universally agreed-upon definitions, can help by providing valuable guidance for establishing basic security practices and building resilience against cyberattacks. This intersected but holistic approach to data protection and cybersecurity can really foster an enhanced security in the digital environment of the Union, through the technical application of measures, as they derive from legal obligation of the GDPR and NIS Directive.

PART II: CHALLENGES, LIMITATIONS AND FUTURE DIRECTIONS OF DIGITAL SECURITY IN THE EUROPEAN UNION

CHAPTER A: THE IMPACT OF THE LEGAL ORDER OF THE EUROPEAN UNION ON CYBERSECURITY

1. The Principle of Conferral and its Limitations on the Scope of Cybersecurity

The ongoing interaction of the digital and physical environments, which can be attributed to a big extent to the so-called 'Internet of Things' ('IoT') is progressively getting bigger. Even though there is much ambiguity with regard to the definition of IoT in parallel with the notion of cybersecurity and cyber hygiene, as explained above, IoT can be understood as the internet-connected devices engaging with physical reality through sensors on a regular basis.[155] Taking into account that the number of such connected devices will reach 25 billion globally by 2025[156], we can expect the distinction between the digital and physical environments will get more blurred.

In this regard, the notion of cybersecurity and its related concepts like cyber resilience and cyber hygiene, is constantly evolving. Although cybersecurity has become critical for the protection of individuals in the digital environment, current EU legislation does not recognize an independent 'right to cybersecurity', nor is it formally mentioned as a policy area in the Treaties. Due to the absence of a clear legal basis for EU related policy in the field of cybersecurity, the Union's competencies are defined but also restricted both in scope and substance, in line with the principle of conferral, as outlined in Article 5 of the Treaty on European Union ('TEU')[157]. Article 5 para. 1 TEU states that '*the limits of Union competences are governed by the principle of conferral*', while para. 2 continues by emphasizing that '*under the principle of conferral, the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Competences not conferred upon the Union in the Treaties remain with the Member States*'. It is clear that under the principle of conferral, the EU can only legislate within the scope of the powers that its Member States have granted it through the Treaties, as specified in Articles 2–6 of the Treaty on the Functioning of the European Union.[158] Therefore, any competences not conferred to the EU by the Treaties remain entirely with the Member States.

While the EU has the capacity to legislate in areas where it is more effective than the Member States on their own, any legislative measure at the EU level, including those related to

[155] Recital 14 of the EU Commission's Data Act proposal can be used as a very useful reference for defining the term Internet of Things (IoT), so as to eliminate the current definitional ambiguity, especially taking into account the IoT will be regulated under the Data Act. IoT refers to '*physical products that, through their components, acquire, generate, or collect data related to their performance, usage, or environment, and are capable of transmitting that data via a publicly accessible electronic communications service*.'

[156] GSMA, "The Internet of Things by 2025" <https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf> accessed 23 September 2024.

[157] Consolidated version of the Treaty on European Union (TEU) [2012] OJ C326.

[158] Paul Craig and Grainne de Burca, EU Law: Text, Cases, and Materials (Oxford University Press 2020), 113.

cybersecurity, must be legally justified, meaning a legal basis must be provided. Specifically, a legislative proposal must meet the criteria outlined in Article 5 TEU, which requires that the legislative measure must either (1) '*not be sufficiently achievable by Member States, whether at central, regional, or local level*', or (2) '*due to the scale or effects of the proposed action, be better accomplished at the Union level*'[159]. Since the adoption of the EU Cybersecurity Strategy in 2013, the legal basis for EU policy in the field of cybersecurity has been linked to the functioning of the internal market, as outlined in Article 114 TFEU, which focuses on the harmonization of national regulations related to the establishment and functioning of the internal market. The rationale behind the EU Cybersecurity Strategy on the use of Article 114 TFEU was based on the idea that cooperation between public and private entities with a view to addressing cyber threats, would significantly support the effective functioning of the internal market and enhance the EU's internal digital security, through a reliable European ICT industry, which would reduce Europe's reliance on foreign technologies.[160] The same rationale was used for the adoption of NIS Directive in 2016 and NIS 2 Directive in 2022 with Article 114 TFEU being used as the legal basis[161], a decision that was the only one available considering the principle of conferral and the limited competence that the EU has in security matters.[162]

Since there is no exclusive competence of the EU in the field of cybersecurity, most legal measures on cybersecurity are established in the form of directives that serve as minimal harmonization instruments. Although this allows Member States the freedom to select the form and methods for implementing the requirements outlined in directives, this 'flexibility' could be potentially viewed as a weakness in minimal harmonization.[163] Even though the NIS framework sets the general objectives of EU legislation, each Member State has adapted its cybersecurity strategy according to its own digital threat landscape and legal framework, as cybersecurity measures and risks can vary significantly across countries, due to differences in digital infrastructure, technological development, and sector-specific needs.[164] On the contrary no such applicability matter arises with the application of the GDPR, which as a regulation has general application, is binding in its entirety and is directly applicable in all EU Member States. In order to overcome this obstacle and pave the way for enhanced EU action on the field of cybersecurity, perhaps the idea of a new 'right to cybersecurity' could be assessed.

[159] Article 5 para. 3 TEU.
[160] European Commission, and High Representative (2013) Cybersecurity strategy of the European Union: an open, safe and secure cyberspace.
[161] Recital 1 of Directive (EU) 2016/1148 and Recital 5 of Directive (EU) 2022/2555 respectively.
[162] Gloria González Fuster and Lina Jasmontaite, 'Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights' in Markus Christen, Bert Gordijn and Michele Loi (eds), *The Ethics of Cybersecurity*, vol 21 (Springer International Publishing 2020).
[163] Ibid.
[164] Ibid.

2. The Emergence of a New Right to Cybersecurity and Future Directions

The main research question in this section will primarily address the question of whether a new fundamental right to cybersecurity is necessary in EU law, and if so, why it is needed. Before that, however, one must consider whether the already existing fundamental right to security is sufficient to address the threats of the current cyber environment in the Union on its own. Therefore, a broad reflection on the concepts of security will follow. The first legal question that must be answered with regard to the potential introduction of a new right to cybersecurity in EU law is, whether amending the existing general right to security or broadly interpreting it to include digital contexts, would address cyber threats. Cybersecurity, as explained in Part I, focuses on the protection against digital threats, while security has to do with physical safety. Even though cybersecurity and security share the same linguistic root, they should be treated as two distinct concepts, from which different rights arise.[165] Although two distinct fields, their intersection has become bigger than ever, given the rise of the Internet of Things, which resulted in fading the boundaries of physical and digital world. Today's connectivity across all aspects of society and the market, driven by the IoT, highlights how '*human safety now depends on encryption, authentication, data integrity, availability, and other aspects of cybersecurity*' is needed more than ever.[166] Consequently, risk factors and threats in today's digital-physical environment extend beyond technological infrastructure. Cyberattacks, apart from compromising physical safety and having severe consequences for services, can also violate the fundamental rights of individuals. To this end, traditional concepts of cybersecurity, security, and safety have to be addressed in a more interchangeable manner.[167] To achieve this, we must first consider if the right to security includes protection in the digital environment. Article 6 of the Charter provides that '*everyone has the right to liberty and security of person',* in a sense of physical security. This can be also endorsed from secondary legislation in the field of digital security, which also showcase a distinction between cybersecurity and physical security.

NIS 2 Directive and the Directive on the resilience of critical entities (hereinafter 'CER Directive')[168] were introduced together by the Commission in December 2020 as part of the EU Cybersecurity Strategy for the Digital Decade.[169] The CER Directive focuses on the resilience of critical entities with regard to physical security, without addressing issues of cybersecurity, which is already covered by NIS 2 Directive. However, the CER Directive recognizes the importance cybersecurity has in building resilience of critical entities,[170] as well as the complementary relationship between these two notions. Since the afore-mentioned Directives apply simultaneously, Member States have therefore the obligation of implementing measures under both Directives in a coordinated and cohesive manner.

---

[165] Papakonstantinou (n 44).

[166] Laura Denardis, The Internet in Everything - Freedom and Security in a World with No Off Switch, vol 148 (1st edn, Yale University Press 2020)

[167] Anton Vedder, 'Safety, Security and Ethics' in Anton Vedder and others (eds), Security and Law (Cambridge, Antwerp, Chicago: Intersentia 2020).

[168] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, OJ L 333.

[169] European Commission, and High Representative (2020) The EU's Cybersecurity Strategy for the Digital Decade.

[170] Recital 9 of Directive (EU) 2022/2557.

As evidenced by the above analysis, the right to security does not in fact include cybersecurity. As a result, individuals' secure digital life is neither explicitly nor comprehensively protected by any EU fundamental right.[171] It would be of value to examine if a secure digital environment could be protected under the data protection law regime under the GDPR, but the latter does not govern digital security *stricto sensu*. The GDPR addresses security breaches only insofar as they result in 'an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.'[172] However, breaches of technical and organizational security measures can still cause significant harm to individuals, even when personal data is not directly distorted or even affected. For instance, one of the most important results of cyberattacks are financial losses, such as when devices become unusable due to ransomware attacks that affect system functionality.[173] Therefore, if personal data is not affected, these security breaches do not constitute violations of the right to personal data protection under Article 8 of the Charter. Nonetheless, one could only think whether future EU action in cybersecurity can be solely and exclusively based on Article 114 TFEU, as legislative action under this specific Article requires the presence of obstacles to market functioning.[174] On the other hand, the issue of EU competence remains somehow unsolved, given the enhanced role of national technological sovereignty in the field of cybersecurity.

A fundamental right to cybersecurity would reinforce individuals' idea of a secure digital environment and could, also, provide EU secondary legislation with an independent legal basis. However, it is highly debatable if the amendment of the Charter of Fundamental Rights under Article 48 to include a right to cybersecurity would resolve this issue. Simply amending the EU Charter of Fundamental Rights under the procedure in Article 48 TEU[175] would not suffice, given that Article 6 para. 1 TEU explicitly states that '*the provisions of the Charter shall not extend in any way the competences of the Union as defined in the Treaties*'. Consequently, a new right to cybersecurity under the Charter would not give the EU any new exclusive competence on the field.

Taking everything into consideration, an amendment of the Treaties seems as the only way forward to ensure cybersecurity protection at the highest level within the Union, as such an amendment would grant the EU the mandate to regulate in the field without the need on relying solely on the internal market legal basis under Article 114 TFEU. The revision of the Treaties has been gaining a lot of supporters in the last years, especially after the European Parliament's resolution calling for a Convention to reform the Treaties in June 2022[176], so the inclusion of a new cybersecurity right under the future revision cannot be ruled out.

[171] Pier Giorgio Chiara, 'Towards a Right to Cybersecurity in EU Law? The Challenges Ahead' (2024), Computer Law & Security Review.
[172] Article 4 para. 12 of Regulation (EU) 2016/679.
[173] Chiara (n 165).
[174] ibid.
[175] '*The Treaties may be amended in accordance with an ordinary revision procedure. They may also be amended in accordance with simplified revision procedures'.*
[176] 'Treaty Revision: Is Europe Ready for a Qualitative Leap?' <https://www.robert-schuman.eu/en/european-issues/725-treaty-revision-is-europe-ready-for-a-qualitative-leap> accessed 23 September 2024.

CHAPTER B: IMPLEMENTATION CHALLENGES IN THE DIGITAL MARKET

1. Cybersecurity Awareness for Small and Medium-Sized Enterprises (SMEs)

The global digital environment has played a big role in the establishment and market action of small businesses in the last decade. It resulted in enhancing their market reach and offering new opportunities for growth and their ability to generate profit. However, this increased presence in the tech market has also introduced new security challenges that small businesses must navigate.

Concerning the applicability and scope of NIS 2 Directive, Article 2 explicitly states that rules deriving from the NIS regime apply to public or private entities of a type referred to in the Annexes attached therein, as analysed in Part I, which however qualify as medium-sized enterprises. For reasons of clarity, it has to be mentioned that NIS 2 Directive applies also to other enterprises regardless of their size, in accordance with paragraph 2 of Article 2. The criterion which specifies which enterprises qualify as medium-sized enterprises takes place under Article 2 of the Annex to Recommendation 2003/361/EC[177], or exceed the threshold levels for medium-sized enterprises as stipulated in paragraph 1 of the aforementioned Article, and which provide their services or conduct their activities within the Union. Simultaneously, Article 2 provides for the definition of a medium, small and micro entity. Pursuant to paragraph 1, micro, small, and medium-sized enterprises (hereinafter referred to as 'SMEs') are defined as businesses with fewer than 250 employees, an annual revenue under €50 million, and/or total assets below €43 million. Also in this context, small businesses are characterized by a maximum of 50 employees and a yearly revenue and balance sheet that do not exceed €10 million and lastly a microenterprise is defined as a business with fewer than 10 employees and an annual revenue or balance sheet total that does not surpass €2 million. Even if SMEs are not included in Article 2 and with a first glance it may seem as they remain outside the scope of NIS 2 Directive, that is not entirely true, since other entities that are considered inside the scope of NIS 2 Directive regardless of their size, such as digital service providers, may qualify as SMEs.

Although small in size and revenue, SMEs have a strong position in the economy of the EU. More specifically, 99% percent of businesses in Europe are SMEs.[178] Due to this, it is apparent that SMEs employ a significant portion of the European workforce, providing with accessible jobs millions of European citizens and therefore playing a crucial role in building entrepreneurship across Europe. SMEs usually provide products or services with original features, compared to the products offered by larger and usually multinational companies. Nonetheless, neither their abundance nor their originality could have possibly prevented the financing problem that they are facing.[179] SMEs and other startup companies, almost always encounter financial obstacles that can jeopardize their existence and place in the market, as well as their development.[180] Compared to

[177] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises [2003] OJ L 124

[178] SMEs, European Commission <https://single-market-economy.ec.europa.eu/smes_en> accessed 27 September 2024.

[179] SMEs and Mid-Caps, European Investment Bank <https://www.eib.org/en/projects/topics/sme/index> accessed 27 September 2024.

[180] Simone Boccaletti and others, 'European SMEs' Growth: The Role of Market-Based Finance and Public Financial Support' [2024] Small Business Economics.

larger firms, they have more difficulty in accessing capital and have a less varied list of funding sources.[181] These challenges in funding resulted from a combination of the global financial crisis and the sovereign debt crisis, which followed in the euro area and the COVID-19 pandemic.[182] With regard to the sovereign debt crisis in several countries of the Eurozone, banks' significant holdings of national sovereign bonds, resulted in the banking sectors of struggling countries facing pressure in financial markets, which increased funding costs.[183] Therefore, the allocation of credit to SMEs became even more limited.

The problem is that due to their need for fast development, SMEs adapt their business plans and strategies more quickly than larger companies and as they constantly try to innovate and improve quality, the application of new technologies becomes necessary. However, this application of technological tools, often leads to risks, as SMEs adopt new technologies without conducting a thorough cybersecurity assessment.[184] In practice, SMEs may not fully understand the risks they introduce to their everyday activities or how these changes could affect their overall cybersecurity, making them more vulnerable to cyberattacks and data breaches. This lack of knowledge is usually combined with the misconception that due to their size, they fail to catch the attention of cybercriminals, as they believe cybercriminals are more attracted to larger businesses and can gain more profit from attacking them, instead the smaller ones.[185] This idea is in fact wrong, since cybercriminals find it relatively easier to attack smaller business, which on the other hand, often conduct business and rely on the services of larger and usually multinational companies, and therefore allowing for cyberattacks to reach larger schemes with less effort.[186] All these elements make SMEs underestimate the importance of installing proper cybersecurity measures and fail to include cybersecurity as a foundation for their business plans and systems, despite the growing threat.

In order to better understand the threat that SMEs are facing, statistics show that 43% of SMEs were a victim of cyberattacks in 2023 alone[187], while the cost of a data breached through phishing emails and malware amounted approximately to 4,000€[188]. The most important statistic,

---

[181] Ibid.

[182] Katarzyna Bańkowska, Annalisa Ferrando and Juan Angel García, 'Access to Finance for Small and Medium-Sized Enterprises after the Financial Crisis: Evidence from Survey Data' <https://www.ecb.europa.eu/press/economic-bulletin/articles/2020/html/ecb.ebart202004_02~80dcc6a564.en.html> accessed 27 September 2024.

[183] Ibid.

[184] Sunil Chaudhary, Vasileios Gkioulos, David Goodman, Cybersecurity Awareness for Small and Medium-Sized Enterprises (SMEs): Availability and Scope of Free and Inexpensive Awareness Resources, Computer Security. ESORICS 2022 International Workshops: CyberICPS 2022, SECPRE 2022, SPOSE 2022, CPS4CIP 2022, CDT&SECOMANE 2022, EIS 2022, and SecAssure 2022, Copenhagen, Denmark, September 26–30, 2022, Revised Selected Papers, vol 13785 (Springer International Publishing 2023).

[185] European Commission, Supporting Specialised Skills Development: Big Data, Internet of Things and Cybersecurity for SMEs : Executive Summary (Publications Office of the European Union 2020) <https://data.europa.eu/doi/10.2826/84436> accessed 27 September 2024.

[186] U.S. Securities and Exchange Commission: The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses <https://www.sec.gov/news/statement/cyb ersecurity-challenges-for-small-midsize-businesses.html> accessed 27 September 2024.

[187] Amal Khalifa Al Aamer and Allam Hamdan, Cyber Security Awareness and SMEs' Profitability and Continuity: Literature Review, Rim El Khoury and Nohade Nasrallah (eds), *Emerging Trends and Innovation in Business and Finance* (Springer Nature Singapore 2023) <https://link.springer.com/10.1007/978-981-99-6101-6> accessed 24 September 2024.

[188] Ibid.

though, that showcases the severity of these attacks for SMEs, is the fact that 60% of SMEs that suffered a cyberattack ceased operations after only six months of the occurring of the attack.[189]

As mentioned above already, one of the primary reasons SMEs are more prone to cyberattacks is their limited funding and assets. Due to this, they often do not hire or pay for services of specialized IT personnel, which will help build their system and apply appropriate technical security measures. To confirm this, evidence show that 58% of SMEs do not even have a cybersecurity plan, which they follow and implement.[190] Studies have found that SMEs do not have a proactive approach to cybersecurity, but rather a reactive one, neglecting applying security measures, until they experience a breach. This late reacting approach results from the lack of understanding of the risks involved and the following failure to create a cybersecurity culture, even though a strong security business mindset is considered the best way to tackle factors that weaken cybersecurity. Building and investing in a cybersecurity culture based on knowledge, perception and business behaviour is essential for marking improvement, staying safe while conducting business and transactions, as well as earn the trust of bigger shareholders that can invest in SMEs.

Apart from lack of security action, the most usual vulnerability for SMEs is human error.[191] Lack of education on behalf of employees undermines security in a way that is almost never noticeable and usually has the form of weak passwords, answering to phishing emails, handling data in a way that leads to loss, destruction or even disclosure. Even if there a basic security policy within the business, the overall lack of approach to security makes it hard for personnel to deeply understand the requirements of handling software and hardware. It is important that the approach that SMEs will take with regard to security to be a holistic one, which starts from the early stages of business activities and stretches to employee training. Employees should at least understand and develop minimum security awareness, be familiar with the organization's security policies and procedures, and be aware of the potential consequences of their actions.[192]

Taking into account the importance of employee behavior and the role it can play in undermining cybersecurity safeguards and overall cyber hygiene, SMEs must prioritize system development, drafting guidelines and policies concerning good cyber practices and of course need employee training, so as to ensure that the personnel are well-trained and up-to-date with regard to handling data and other sensitive information. Nonetheless, in order to mitigate the cyber risks, an important amount of funding and resources is needed. This creates a vicious cycle, according to the lack of funding that was explained above. Given the financial damage and loss due to cyberattacks, which can get bigger and bigger due to lack of resources for cybersecurity, we need to examine the alternatives the SMEs have. The following paragraphs will consist of the alternatives that SMEs have in accessing funding, that will help them mitigate the constantly arising cyberthreats. As our focus is shifted towards the European market, we will primarily examine the funding that comes directly through the EU.

Researching on the EU alternatives have shown that there are a lot of free and inexpensive trainings and materials on cybersecurity awareness that SMEs can have access to. These packs usually include information on how to detect phishing emails, how to properly protect information, where and how to store passwords and security keys, as well as overall GDPR awareness training.

---

[189] National Security Alliance, Cybersecurity Awareness Month - National Cybersecurity Alliance <https://staysafeonline.org/programs/cybersecurity-awareness-month/> accessed 27 September 2024.
[190] Amal Khalifa Al Aamer and Allam Hamdan (n.181).
[191] Ibid.
[192] Ibid.

In particular, ENISA has created and is offering an '*Awareness Raising in a Box (AR-in-a-BOX)'*, which is designed to help essential entities, large organizations, as well as SMEs, build and establish cybersecurity awareness activities and training within their business.[193] *AR-in-a-BOX* includes guidelines for creating awareness campaigns for internal and external activities, selecting appropriate tools and how to handle them internally, measuring program effectiveness, developing security strategies and learning material.[194] On the other hand, EUROPOL also shares similar assistance through the European Cybercrime Centre ('EC3'). The EC3 manages to effectively raise awareness of cybercrime to the public and private sector, by providing information and training on how to prevent and detect threats.[195] In addition, it distributes educational material, such as brochures, infographics and videos, that can be used by businesses in order to understand how cyberattacks take place, the steps to take in case they happen and general best practices for online safety.[196]

The European Digital SME Alliance, a networking group of SMEs that cooperate closely with the European Commission with a view to supporting digital SMEs in Europe, also provides and distributes materials on cybersecurity concerns relevant to SMEs.[197] The most interesting and in many ways helpful asset that the European Digital SME Alliance provides a guide on how SMEs can implement '*the most important cybersecurity standard'*[198] as they call it within the network, the ISO/IEC 27001 standard[199], as explained in Part I. At the same time, the European Maritime Safety Agency ('EMSA') offers cybersecurity training especially built and designated for the maritime sector.[200]

Furthermore, these EU agencies organize a variety of cybersecurity events, in order to create a welcoming environment to cybersecurity awareness among EU organizations, but also EU citizens, that are also the ultimate beneficials of cybersecurity business practices. These events include among others the European Cybersecurity Month ('ECSM') organized by ENISA, which is the EU's annual cybersecurity awareness campaign, that takes place through workshops and conferences and aims to educate EU citizens and organizations on how to effectively protected themselves and their operations from online threats.[201] More examples, include the European Conference on Transport Cybersecurity, as well as the Symposium on Global Cybersecurity.

Organised by ENISA, as well, the European Transport Cybersecurity Conference explores strategies helping build a better safety net for European transport against cyberattacks. In fact, the transport sector is the third sector most vulnerable to cyberattacks and even though there are no serious incidents that can be described, attacks can have a serious impact on disruptions,

---

193 ENISA - Cybersecurity Awareness Raising: Peek Into the ENISA-Do-It-Yourself Toolbox <https://www.enisa.europa.eu/news/cybersecurity-awareness-raising-peek-into-the-enisa-do-it-yourself-toolbox> accessed 27 September 2024.

194 Ibid.

195 EUROPOL - European Cybercrime Centre - EC3' <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3> accessed 27 September 2024.

196 Ibid.

197 European DIGITAL SME Alliance, Cybersecurity & Data Protection <https://www.digitalsme.eu/cybersecurity-and-data-protection/> accessed 27 September 2024.

198 Ibid.

199 ISO/IEC 27001 (n. 126).

200 European Maritime Safety Agency, Awareness in Maritime Cybersecurity <https://www.emsa.europa.eu/we-do/safety/maritime-security/item/3477-cybersec.html> accessed 27 September 2024.

201 ENISA - European Cybersecurity Month <https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/european-cyber-security-month> accessed 27 September 2024.

losses and most importantly the safety of EU passengers.[202] The Symposium on Global Cybersecurity Awareness, on the other hand, is co-organised by EUROPOL and the Anti-Phishing Working Group ('APWG')[203] event unites cybersecurity professionals, government officials and industry executives from across the globe to discuss possible ways to tackle the urgent issues of digital security.[204] Many of the above mentioned resources are freely available or require just a brief registration process and can be downloaded without any unnecessary difficulties. They mostly build awareness and resilience by focusing on teaching SMEs how to firstly identify, then detect and lastly protect against cyberattacks. Some of them address also how to respond and recover after a cyberattack or data breach by providing guidance for recovering from ransomware attacks, for instance.

All in all, the lack of funding for SMEs in a general context imposes threats on their 'cyber health', as SMEs lack the knowledge and training to protect their operations from threats or given their small size, they believe they will not catch the attention of attackers. But this is far from being correct. SMEs face more threats than anticipated and if they do not apply appropriate technical safeguards, not just their operation, but their whole existence and development is at stake.

2. The Interplay of Lobbying, Market Competition and the GDPR

Following the analysis provided in Part I, the GDPR is central to the EU's digital privacy legislation and has created positive results by improving the protection for digital service users and protecting the rights of data subjects. It is clear that the GDPR provides benefits for businesses, especially within Europe as well, but also worldwide, since its impact on data protection and privacy has become the global standard.[205] The main organizational advantages of GDPR include among others strong data security practices, which on their turn lower the risk of costly data breaches. Non-compliance on the other hand, can lead to fines of up to €20,000,000 or 4% of the company's total global annual revenue, whichever is greater, as dictated by Article 83 para. 5 of the GDPR, making adherence to data protection rules under the regime of the GDPR critical for minimizing financial risk.

In addition to that, GDPR requires organizations to show accountability in the way they handle data through documentation, audits, and data protection impact assessments, resulting in better internal governance. It is clear, therefore, that the benefits of GDPR compliance are substantial. However, research shows that, while the above is true, evidence also indicates that the GDPR favors big tech companies over smaller businesses.[206] The GDPR appears to have been the

[202] ENISA - 1st Transport Cyber Security Conference <https://www.enisa.europa.eu/events/first-transport-cyber-security-conference> accessed 27 September 2024.
[203] The APWG is an international nonprofit organization committed to fighting phishing and other types of online fraud, such as scamming.
[204] APWG - Global Symposium on Cybersecurity Awareness <https://education.apwg.org/safety-messaging-convention/overview/awareness-symposium> accessed 27 September 2024.
[205] Roxana Vatanparast, 'Designed to Serve Mankind? The Politics of the GDPR as a Global Standard and the Limits of Privacy', 80(4) Heidelberg Journal of International Law 819-845 (2020).
[206] Bartlomiej Chomanski and Lode Lauwaert, 'Digital Privacy and the Law: The Challenge of Regulatory Capture' [2024] AI & SOCIETY.

product of significant lobbying[207] efforts, especially during its drafting stage, with its outcomes favoring big and established tech market businesses at the expense of smaller ones.[208] Lobbying, in the form of influence to the EU institutions by tech giants through advocates of the industry, played a big role in the GDPR's development.[209] Naturally, these personal ties between regulators in EU level and the tech industry, especially considering that most of *Meta*'s and *Google*'s lobbyists were officials at an EU body in the past, are evident.[210] There is therefore a big suggestion that the GDPR's provisions were strategically influenced by business interests within the tech market.

Even though tech companies may lobby against regulatory proposals that regulate their field, they simultaneously recognize the benefits a regulated market and environment holds, since clear market rules can foster consumers' protection and trust between them and the business, as well as create more predictable business transactions.[211]As *Microsoft*'s John Frank noted, multinational companies such as *Microsoft* are not seeking to operate without any oversight and '*are not trying to remain unregulated'*[212]. It is a fact that, clear consumers' protection rules or regulations of any type in general, can reassure consumers and promote trust in products. It seems as this creates a 'safety net' for consumers by dictating that an industry business is in fact compliant with all regulations, therefore enhancing security and accountability.

Another tech giants advocating for regulation include Sam Altman, CEO of *OpenAI*[213] and Mark Zuckerberg of *Meta*, who emphasized that '*he doesn't think private companies should make so many decisions alone when they touch on fundamental democratic values'* and '*people need to feel that global technology platforms answer to someone, so regulation should hold companies accountable when they make mistakes'*[214].

While it might seem surprising that large companies would seek more regulation on their own, at the same time they can benefit by adhering to high standards of regulatory scope, given that they can enhance their reputation within the market, gain consumer trust and differentiate themselves in the marketplace. Nonetheless, compliance with EU regulations can most of the times impose significant costs, especially on small and medium-sized enterprises, while large multinational corporations such as *Google* or *Meta*, with greater resources and market shares, have a distinct advantage in complying with these regulations.[215] This can help them strengthen their

[207] According to Britannica, *lobbying* refers to any effort by individuals or private interest groups to influence government decisions. It could be also understood as the act of advocating for, opposing, or otherwise attempting to influence the introduction of legislation in any legislative body.

[208] Damien Geradin, Dimitrios Katsifis and Theano Karanikioti, 'GDPR Myopia: How a Well-Intended Regulation Ended up Favoring Google in Ad Tech' [2020] SSRN Electronic Journal <https://www.ssrn.com/abstract=3598130> accessed 24 September 2024.

[209] Jockum Hildén, 'Lobby In/Policy Out? Assessing Lobbyist Influence on the GDPR' (2021) 7 European Data Protection Law Review 520.

[210] 'The Revolving Door – from Public Officials to Big Tech Lobbyists | Corporate Europe Observatory' <https://corporateeurope.org/en/2022/09/revolving-door-public-officials-big-tech-lobbyists> accessed 24 September 2024.

[211] Bradford A, The Brussels effect: how the European Union rules the world. Oxford University Press, New York, 2020

[212] Chomanski and Lauwaert (n 200).

[213] Cecilia Kang, 'OpenAI's Sam Altman Urges A.I. Regulation in Senate Hearing' *The New York Times* (16 May 2023) <https://www.nytimes.com/2023/05/16/technology/openai-altman-artificial-intelligence-regulation.html> accessed 24 September 2024.

[214] 'Big Tech Needs More Regulation' (*Meta*, 18 February 2020) <https://about.fb.com/news/2020/02/big-tech-needs-more-regulation/> accessed 24 September 2024.

[215] Chomanski and Lauwaert (n 200).

market position, potentially hindering the growth of smaller rival companies by receiving more public attention. Therefore, the real hidden cost of EU regulations, including the GDPR, is borne by smaller businesses, which usually struggle to meet the strict regulatory requirements and compete effectively.

When referring to implementation cost according to the GDPR,, for the purpose of the present thesis, we are referring to the cost of applying technical and organizational safeguards with regard to security, as analyzed in Part I. The costs that the establishment of privacy by design requires is relatively high, especially if one considers privacy within the general context of privacy-preserving and privacy-enhancing technologies, designed to safeguard sensitive data, while preserving the confidentiality and integrity of information. In order to have an *a priori* consideration of how to properly and effectively integrate data protection principles into the designing and construction of information and communication technology systems, including hardware, software, networks and data storage, in order to enhance privacy, extensive training on privacy requirements under the current legislative framework on behalf of developers must take place, the cost of which is relatively high. It is highly doubtable that SMEs can have such costly trainings for their developers, while even the compliance with 'easier' –if this is the correct term- rules and obligations with regard to the processing of data seems financially burdening.[216]

If multinational companies can invest between $30 million and $50 million in customer databases as part of their strategy to comply with GDPR regulations[217], and as a result build a strong sense of trust within the market, then GDPR compliance would have successfully increased market concentration in the data market in their hands, potentially harming smaller firms and limiting competition.[218] This general scheme is evident that does not benefit smaller tech businesses. For instance, the requirement to obtain user consent for data usage under Article 6 of the GDPR has certain transaction costs on internal data collection, affecting more and at a disproportionate level smaller or newer firms.[219]

In addition to the above, it could be argued that the GDPR introduces uncertainty. But this should be further explained in depth. Uncertainty is created because individuals often exhibit ignorance and indifference regarding their digital privacy and have generally little awareness about why and most importantly how their personal data is stored, collected or even transferred.[220] Specifically, end-users do not read privacy notes or if they do, they usually do not understand them, especially if the issues explained are of technical nature. Another aspect of the problem is when they both read and understand them, they often lack information to make to make decisions. At a first glance, a solution to this problem would be the principle of transparency under Article 5 of the GDPR, which mandates that processing activities must be thoroughly communicated to data

[216] 'The EU Data-Protection Regulation—Compliance Burden or Foundation for Digitization? | McKinsey' <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-eu-data-protection-regulation-compliance-burden-or-foundation-for-digitization> accessed 25 September 2024.
[217] Ibid.
[218] Johnson G., Economic research on privacy regulation: lessons from the GDPR and Beyond. National Bureau of Economic Research Working Paper Series No. 30705, 2022.
[219] Campbell J, Goldfarb A, Tucker C, Privacy regulation and market structure, J Econ Manag Strategy (2015), 47–73
[220] Manuel Rudolph, Denis Feth and Svenja Polst, 'Why Users Ignore Privacy Policies – A Survey and Intention Model for Explaining User Privacy Behavior' (2018).

subjects in a clear and accessible manner to ensure they understand how their data will be used.[221] Transparency in processing requires the use of straightforward and plain language, in order for end-users to be explicitly informed about the rules and safeguards, which surround the processing of their personal data.[222] On a second glance, of course the principle of transparency would be a good base for end-users to understand and give consent with more confidence, but the problem requires a more holistic approach – one that includes appropriate basic knowledge on behalf of individuals concerning their privacy rights.

Thus, under this uncertainty, there can be an indirect and underlying influence to individuals, making them more inclined and confident to share their data with large and well-established companies.[223] In turn, this uncertainty can further concentrate the data market in a few, multinational companies and limit competition between large and small business, at least until end-users' confidence and knowledge in the possible ways the processing of their data takes place, improves. Research has, also, shown that *Google*'s market share increased after the introduction of the GDPR, while some of its competitors suffered serious losses, somehow proving the above suggestions that the GDPR may have benefited larger companies like *Google*[224]. In markets, such as the digital market, where data is in fact the driving force, consent and cookies management under the GDPR is easier within a single large company, which does not necessarily share data with third parties, but process it on its own. As a result, the GDPR has fostered an environment where data sharing within the same firm is considered less risky than sharing with third-parties.[225]

Moreover, website providers may prefer larger digital businesses to reduce their own compliance risks, as these providers have more resources to handle legal challenges, following the same rationale in trust building within the market that individuals have. Connected to the afore-mentioned input in the cost of privacy by design, the GDPR's increased costs for app developers, leading to reduced innovation and fewer app being ultimately developed.[226] This ultimately harmed consumers by limiting market choices and reducing consumer-producer surplus. While no one can deny that the long-term benefits of the GDPR for big tech giants remain uncertain, the extensive lobbying suggests that large companies enjoy current benefits, which the GDPR has likely set the conditions for.[227]

While privacy groups, scholars and regulators focus on consumer privacy, privacy industry prioritizes business profits. Nonetheless, end-users and the public in general may not be as concerned with corporate profits or digital privacy at all. Therefore, the overall advocacy and lobbying that value digital privacy, occur more than the average individual's efforts, in protecting their data online and this suggests that their priorities may differ from those of the general public. While people may want greater control over their digital data, it's unclear whether they fully understand the regulations around it. The GDPR offers this protection without much effort on behalf of individuals – given that their involvement is limited, but at the same time it maximizes

[221] European Union Agency for Fundamental Rights and Council of Europe (n 67).
[222] Ibid.
[223] Chomanski and Lauwaert (n 200).
[224] Christian Peukert and others, 'Regulatory Spillovers and Data Governance: Evidence from the GDPR' (2022) 41 Marketing Science 746.
[225] Ibid.
[226] Ibid.
[227] Mitnick B. Capturing 'capture': definition and mechanisms, (2011), Handbook on the Politics of Regulation, Elgar Publishing, Cheltenham, p. 35–49

the cost for end-users, who end up having limited options in the tech industry, given the current state of market competition, due to implementation cost. The main issue is not simply whether people want more privacy protection, but also whether they are willing to accept the high cost of choosing products of big tech companies. Naturally, it remains unclear whether people value privacy enough to justify these costs and unfortunately '*we cannot assume that privacy is always the most important value*'[228], as Chomanski and Lauwaert explained.

Interim conclusion

In conclusion, while the GDPR has made significant efforts in enhancing user privacy and strengthening data protection application, it also poses challenges that affect smaller businesses at a disproportionate level. Although it aims to foster consumer trust and establish standards in the protection of personal data, the compliance costs can interfere with innovation and market competition, putting larger tech companies at an advantage that can navigate the regulatory landscape more easily due to their financial assets. This situation is also maintained by a general lack of awareness among users regarding their privacy rights, leading to a reliance on established companies in the market.

Moreover, SMEs in Europe are particularly vulnerable to cyberattacks, which can threaten their operations and even existence, due to insufficient funding and cybersecurity knowledge. Fortunately, there are accessible resources from the EU aiming to assist SMEs in enhancing their cybersecurity awareness. However, the EU funding cannot solve the problem on its own, without a more targeted approach on SMEs specifically. What is needed is a less costly approach on cybersecurity, which cannot be solved on a regulatory level.

Lastly, the analysis of this chapter has resulted in enhancing the idea that the establishment of a new 'right to cybersecurity' could create a more stable and strong legal framework, allowing for effective regulation and fostering a uniform digital landscape across Member States. This would allow for the effective balance between user privacy and the following protection of fundamental rights, with the need for a competitive digital market, ensuring that both businesses and consumers can thrive in a fast-evolving technological environment within the Union.

[228] Chomanski and Lauwaert (n 200).

CONCLUSION

Taking everything into consideration, the digital revolution has undoubtedly transformed our daily lives, offering an abundance of opportunities for connectivity, transactions and of course, economic growth. From the creation of the internet to the rise of e-commerce, the digital age has reshaped how people communicate, work and interact and new technologies, such as AI and cloud computing have further accelerated this transformation, creating room for enhanced efficiency and productivity across various sectors. However, as mentioned in the beginning of this thesis, this transformation has also brought about significant challenges, particularly in the sector of data protection and cybersecurity, as more personal information is shared online and as businesses rely more and more on digital platforms for their operations. Therefore, the risks associated with data breaches, cyberattacks, and identity theft have intensified.

In response to threats, the European Union has taken measures steps to address these challenges through legislation, with a view to creating a secure digital environment. These efforts were made in order to safeguard fundamental rights but also the proper functioning of the internal market, through rules that will apply to businesses under the GDPR and NIS 2 Directive. The scope of this thesis was the examination of the interplay between data protection principles and cybersecurity, measures as outlined in the GDPR and NIS 2 Directive, given that these two legislative measures have set high standards for protecting personal data and building cybersecurity across the European Union. The GDPR, implemented in 2018, introduced enhanced requirements for how organizations collect, process and store personal data and its primary objective is to safeguard the privacy rights of individuals by granting them more control over their personal information. On the other hand, the NIS 2 Directive focuses on strengthening the overall cybersecurity scheme of essential and important entities within the EU. It seeks to improve the resilience and capability of network and information systems by mandating a higher level of cybersecurity measures among operators of essential services and other entities that have obligations under it.

Throughout this research, we have analyzed the legal obligations imposed on businesses and organizations to implement appropriate technical and organizational safeguards to protect personal data and enhance cybersecurity. For instance, under the GDPR, organizations must adopt measures such as data encryption, risk assessments, and employee training programs to ensure compliance. Similarly, the NIS 2 Directive requires organizations to implement risk management practices, incident reporting policies and measures such as encryption within the organization.

While these regulations provide a solid foundation for digital security in the EU, their practical application has revealed certain shortcomings and challenges that cannot be overlooked. One of the key findings of this topic is the need for a more comprehensive approach to digital security. While the GDPR and NIS 2 provide valuable guidance, their overlapping requirements can create confusion and hinder effective implementation. For example, the GDPR emphasizes the need for privacy by design, which one could argue that it is in fact a NIS 2's requirement for mitigating cyber risks. Such overlapping obligations can lead to uncertainties regarding compliance, placing additional burdens on organizations which try to understand which obligation

comes first and which follows. Perhaps a more unified framework that clearly states responsibilities is essential to ensure maximum protection of in case of attacks.

Furthermore, the fact that SMEs remain out of the scope of NIS 2 Directive, but other entities that are inside its scope regardless of their size, such as digital service providers, may qualify as SMEs, makes us skeptical about the overall level of digital security in Europe. This vulnerability is particularly concerning given that SMEs form a crucial part of the EU economy, representing over 99% of all businesses and employing a significant portion of the European workforce. Therefore, the impact of cyber incidents affecting SMEs is substantial. According to various studies, a significant percentage of SMEs have reported experiencing cyber incidents, but they almost always struggle to respond effectively. The burden of implementing robust cybersecurity measures can be particularly big for smaller organizations with limited resources. Many SMEs lack the financial and technical expertise to invest in advanced security solutions, leaving them vulnerable to cyber threats. It can be understood that with a limited number of resources and such a big percentage of attacks, SMEs have positioned themselves in a difficult situation.

To address this challenge, support and funding initiatives are necessary to help SMEs achieve adequate levels of cyber resilience. EU action can play a vital role in this effort by offering financial assistance, support and training programs specially adapted to the needs of smaller businesses. Initiatives such as the ones offered by ENISA aim to enable them to adopt effective cybersecurity measures, while minimizing financial burden. By providing resources that help SMEs understand the risks they face and the importance of compliance with regulations like GDPR and NIS 2, the EU can empower them to take proactive measures to protect their digital assets and market place. In addition to financial support, raising awareness about data protection application is crucial for SMEs, especially since regulations like the GDPR favor big tech companies over smaller ones. Many small businesses are unaware of the risks they face or the obligations imposed by GDPR and NIS 2, so effective programmes designed to the specific needs of smaller organizations can enhance their understanding of regulatory compliance and help them implement best practices in data protection and cybersecurity.

Moreover, research findings have highlighted the importance of collaboration among stakeholders, including regulators, businesses, and experts. A collaborative approach can facilitate the sharing of knowledge, resources, and best practices, ultimately enhancing the overall cybersecurity and data protection posture of the digital environment. For instance, public-private partnerships can provide valuable insights of threats and enable organizations to develop more effective responses. These collaborations can also make room for innovation by bringing together diverse perspectives and expertise to tackle cyber challenges. By promoting information sharing and coordinated responses to cyber incidents, business strategies will create a more resilient digital environment. This collaborative framework will be deemed crucial for addressing the dynamic and interconnected nature of cyber threats, as attackers often exploit vulnerabilities across multiple sectors and jurisdictions.

Additionally to enhancing collaboration, the thesis recognizes the role of technological innovation in improving cybersecurity and data protection. Emerging technologies, such as artificial intelligence and machine learning, often offer new possibilities for enhancing security measures. For instance, AI can be utilized to analyze vast amounts of data in real-time, detecting

risks and potential threats more efficiently than traditional methods. By using these technologies, organizations can boost their defenses and respond to incidents more effectively. However, the integration of new technologies also raises important regulatory considerations that must be addressed to ensure compliance with data protection laws. Furthermore, the need for ongoing dialogue between regulators and the tech industry must be emphasized. As technology evolves rapidly, regulatory frameworks must adapt accordingly.

By engaging with industry stakeholders, regulators can gain valuable insights into the challenges and opportunities presented by new technologies. This dialogue can result in the development of regulations that strike a balance between innovation and ensuring effective protection of personal data and cybersecurity. By fostering this collaborative approach between regulators, businesses, and stakeholders, the EU can create a digital landscape that balances innovation with the protection of fundamental rights. Policymaking in the EU must monitor the effectiveness of existing regulations and be willing to adjust them in response to changing technological innovations that may put in danger fundamental rights. Additionally, investing in research and development to stay ahead of cyber threats will further strengthen the digital security framework.

Ultimately, creating a secure digital environment is not solely the responsibility of regulators; it requires the active participation of all stakeholders involved. By recognizing the shared responsibility in safeguarding personal data and enhancing cybersecurity, the EU can work towards building a more resilient digital landscape that promotes innovation while ensuring the proper functioning of the internal market as well. In summary, the path forward involves a commitment to collaboration, education and a willingness to adapt to the fast-changing digital landscape. Through these efforts, the EU can ensure that the benefits of the digital revolution are met, while minimizing the risks associated with cyber threats. In doing so, it will foster an environment of trust and security that enables individuals and organizations to thrive in the digital age.

Additionally, as the global landscape continues to evolve, international cooperation in cybersecurity becomes increasingly important. Cyber threats are not confined by borders, and attackers often operate in a transnational context, making it important for nations to work together to combat these challenges. The EU can take a leading role in fostering international partnerships, aimed at enhancing global cybersecurity efforts. It has done this already by developing the world standard in data protection, through the GDPR. By sharing best practices, information, and intelligence, countries can create a united front against cyber threats that jeopardize not only individual nations but also the stability of the global digital economy.

In conclusion, the European Union's efforts to establish a secure digital environment through the GDPR and NIS 2 are commendable. However, the rapidly evolving nature of cyber threats and the complexities of implementing these regulations necessitate ongoing evaluation and adaptation.

REFERENCES

LEGISLATION OF THE EUROPEAN UNION

A. PRIMARY LEGISLATION

Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

Consolidated version of the Treaty on European Union (TEU) [2012] OJ C326

Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47

B. SECONDARY LEGISLATION

Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises [2003] OJ L 124

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) [2016] OJ L 194

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L 333

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, OJ L 333

Directive 95/46/EC of the European Parliament and of 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 [1995] OJ L281/31.

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) [2016] OJ L119/1

EUROPEAN UNION'S DOCUMENTS AND SOURCES

Data Protection Working Party Opinion 04/2007 on the concept of personal data [2007] 01248/07/EN WP 136

ENISA - Cybersecurity Awareness Raising: Peek Into the ENISA-Do-It-Yourself Toolbox <https://www.enisa.europa.eu/news/cybersecurity-awareness-raising-peek-into-the-enisa-do-it-yourself-toolbox> accessed 27 September 2024.

European Agency for Cybersecurity, Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies, 2016.

European Commission, and High Representative (2013) Cybersecurity strategy of the European Union: an open, safe and secure cyberspace.

European Commission, and High Representative (2013) Cybersecurity strategy of the European Union: an open, safe and secure cyberspace.

European Commission, and High Representative (2020) The EU's Cybersecurity Strategy for the Digital Decade.

European Union Agency for Cybersecurity., Data Pseudonymisation: Advanced Techniques and Use Cases : Technical Analysis of Cybersecurity Measures in Data Protection and Privacy. (Publications Office 2021) <https://data.europa.eu/doi/10.2824/860099> accessed 8 September 2024.

European Union Agency for Fundamental Rights and Council of Europe (ed), Handbook on European Data Protection Law (2018 edition, Publications Office of the European Union 2018).

European Union Agency for Network and Information Security, Review of Cyber Hygiene Practices. (Publications Office 2016) <https://data.europa.eu/doi/10.2824/352617> accessed 20 September 2024.

EUROPOL - European Cybercrime Centre - EC3' <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3> accessed 27 September 2024.

EU Cybersecurity Initiatives: Working towards a More Secure Online Environment | Shaping Europe's Digital Future' (5 July 2016) <https://digital-strategy.ec.europa.eu/en/library/eu-cybersecurity-initiatives-working-towards-more-secure-online-environment> accessed 1 September 2024.

How Do EU Citizens Manage Their Personal Data Online?' <https://ec.europa.eu/eurostat/web/products-eurostat-news/-/edn-20220127-1> accessed 4 September 2024.

Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM/2020/823).

SMEs, European Commission <https://single-market-economy.ec.europa.eu/smes_en> accessed 27 September 2024

SMEs and Mid-Caps, European Investment Bank <https://www.eib.org/en/projects/topics/sme/index> accessed 27 September 2024.

CONVENTIONS

Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data [1981] ETS 108

Council of Europe, Convention on Cybercrime [2001] ETS 185

JUDGMENTS

Judgment of the Court (Grand Chamber), 8 April 2014, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, ECLI:EU:C:2014:238.

Judgment of the Court (Fourth Chamber), 11 December 2014, Case C-212/13, František Ryneš v Úřad pro ochranu osobních údajů, ECLI:EU:C:2014:2428.

Judgment of the Court (Grand Chamber) of 16 July 2020, Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559

Judgment of the Court (Second Chamber) of 19 October 2016, Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland, ECLI:EU:C:2016:779.

Judgment of the Court (Second Chamber) of 20 December 2017, Case C-434/16, Peter Nowak v Data Protection Commissioner, ECLI:EU:C:2017:994.

Judgment of the General Court (Eighth Chamber, Extended Composition) of 26 April 2023, Case T-557/20, Single Resolution Board v European Data Protection Supervisor, ECLI:EU:T:2023:219.

BIBLIOGRAPHY (TEXTBOOKS, ARTICLES AND PAPERS)

Amal Khalifa Al Aamer and Allam Hamdan, Cyber Security Awareness and SMEs' Profitability and Continuity: Literature Review, Emerging Trends and Innovation in Business and Finance (Springer Nature Singapore 2023).

Ann Cavoukian, 'Privacy by Design The 7 Foundational Principles', Implementation and Mapping of Fair Information Practices.

Anton Vedder, 'Safety, Security and Ethics' in Anton Vedder and others (eds), Security and Law (Cambridge, Antwerp, Chicago: Intersentia 2020).

Arun Vishwanath and others, 'Cyber Hygiene: The Concept, Its Measure, and Its Initial Tests' (2020) 128 Decision Support Systems 113160.

Back End: A Complete Overview on Its Relevance in Data Science' <https://datascientest.com/en/all-about-back-end> accessed 13 September 2024.

Background and Evolution of the EU General Data Protection Regulation (GDPR) | The EU General Data Protection Regulation (GDPR): A Commentary | Oxford Academic' <https://academic.oup.com/book/41324/chapter-abstract/352293200?redirectedFrom=fulltext> accessed 27 August 2024.

Background and Introduction to the General Data Protection Regulation' (Lexology, 19 September 2017) <https://www.lexology.com/library/detail.aspx?g=d7f59709-4362-4155-ab6f-de55af4147a4> accessed 27 August 2024.

Bartlomiej Chomanski and Lode Lauwaert, 'Digital Privacy and the Law: The Challenge of Regulatory Capture' [2024] AI & SOCIETY.

Bradford A, The Brussels effect: how the European Union rules the world. Oxford University Press, New York, 2020

Campbell J, Goldfarb A, Tucker C, Privacy regulation and market structure, J Econ Manag Strategy (2015), 47–73

Christian Peukert and others, 'Regulatory Spillovers and Data Governance: Evidence from the GDPR' (2022) 41 Marketing Science 746.

Damian Eke and Bernd Stahl, 'Ethics in the Governance of Data and Digital Technology: An Analysis of European Data Regulations and Policies' (2024) 3 Digital Society 11.

Damien Geradin, Dimitrios Katsifis and Theano Karanikioti, 'GDPR Myopia: How a Well-Intended Regulation Ended up Favoring Google in Ad Tech' [2020] SSRN Electronic Journal <https://www.ssrn.com/abstract=3598130> accessed 24 September 2024.

Denise M Carter, 'Cyberspace and Cyberculture' in Audrey Kobayashi (ed), International Encyclopedia of Human Geography (Second Edition) (Elsevier 2020) <https://www.sciencedirect.com/science/article/pii/B9780081022955108108> accessed 18 September 2024.

Dietmar PF Möller, Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices, vol 103 (Springer Nature Switzerland 2023) <https://link.springer.com/10.1007/978-3-031-26845-8> accessed 15 August 2024.

Donnees personnelles, 'A General Data Protection Regulation For Europe? Light And Shade In The Commission's Draft Of 25 January 2012' [/01/23] SCRIPTed <https://script-ed.org/?p=406> accessed 27 August 2024.

Ewa Luger, Lachlan Urquhart, Tom Rodden and M. Golembewski "Playing the Legal Card: Using Ideation Cards to Raise Data Protection Issues within the Design Process" Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 15), Seoul, 18-23 April 2014.

Felix Bieker and others (eds), Privacy and Identity Management: 17th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Privacy and Identity 2022, Virtual Event, August 30–September 2, 2022, Proceedings, vol 671 (Springer Nature Switzerland 2023) <https://link.springer.com/10.1007/978-3-031-31971-6> accessed 15 August 2024.

Fereniki Panagopoulou-Koutnatzi, 'The General Data Protection Regulation (EU) 679/2016: Introduction and Fundamental Rights Protection' (Sakkoulas, 2017) (translated in English).

Gloria González Fuster and Lina Jasmontaite, ‘Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights’ in Markus Christen, Bert Gordijn and Michele Loi (eds), The Ethics of Cybersecurity, vol 21 (Springer International Publishing 2020).

Grażyna Maria Szpor, ‘The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland’ (2021) 46 Review of European and Comparative Law 219.

Gregory J. Touhill & Touhill, C. Joseph (2014), Cybersecurity for executives: A practical guide, John Wiley & Sons.

Gunderson, L., Holling, C.: Panarchy: Understanding Transformations in Human and Natural Systems. Bibliovault OAI Repository, p. 114. The University of Chicago Press (2003)

Hustinx Peter, ‘EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation’

Ira S Rubinstein, ‘Regulating Privacy By Design’, 2011.

Izzat Alsmadi, The NICE Cyber Security Framework: Cyber Security Intelligence and Analytics (Springer International Publishing 2023) <https://link.springer.com/10.1007/978-3-031-21651-0> accessed 21 September 2024.

Javier Guerrero and others, ‘Encryption Techniques: A Theoretical Overview and Future Proposals’ (2016).

Jerry Andriessen and others (eds), Cybersecurity Awareness, vol 88 (Springer International Publishing 2022).

Jockum Hildén, ‘Lobby In/Policy Out? Assessing Lobbyist Influence on the GDPR’ (2021) 7 European Data Protection Law Review 520.

Johnson G., Economic research on privacy regulation: lessons from the GDPR and Beyond. National Bureau of Economic Research Working Paper Series No. 30705, 2022.

Julio Navío-Marco, ‘Cyberspace as a System and a Social Environment: A Theoretical Proposal Based on Niklas Luhmann’.

KA Taipale, ‘Cyber-Deterrence’ (1 January 2009) <https://papers.ssrn.com/abstract=1336045> accessed 21 September 2024.

Laura Denardis, The Internet in Everything - Freedom and Security in a World with No Off Switch, vol 148 (1st edn, Yale University Press 2020)

Lilian Edwards, ‘Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective’ [2016] SSRN Electronic Journal <http://www.ssrn.com/abstract=2711290> accessed 25 August 2024.

Manuel Rudolph, Denis Feth and Svenja Polst, ‘Why Users Ignore Privacy Policies – A Survey and Intention Model for Explaining User Privacy Behavior’ (2018).

Martina Lindorfer, The Threat of Surveillance and the Need for Privacy Protections (Introduction to Digital Humanism: A Textbook), 2024

Masike Malatji and Alaa Tolah, 'Artificial Intelligence (AI) Cybersecurity Dimensions: A Comprehensive Framework for Understanding Adversarial and Offensive AI' [2024] AI and Ethics.

Mitnick B. Capturing 'capture': definition and mechanisms, (2011), Handbook on the Politics of Regulation, Elgar Publishing, Cheltenham, p. 35–49

Myriam Dunn Cavelty, 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse' (2013) 15 International Studies Review 105, p. 107.

Organisation for Economic Co-operation and Development, 'Inventory of Privacy-Enhancing Technologies (PETs)', 2002.

Paul Craig and Grainne de Burca, EU Law: Text, Cases, and Materials (Oxford University Press 2020), 113.

Paunović, Katarina. "Data Processing and Storage." Encyclopedia of Public Health, edited by Wilhelm Kirch, Springer Netherlands, 2008.

Petar Radanliev, 'Digital Security by Design' [2024] Security Journal <https://link.springer.com/10.1057/s41284-024-00435-3> accessed 15 August 2024.

Peter Chase, 'Perspectives on the General Data Protection Regulation Of the European Union'.

Pier Giorgio Chiara, 'Towards a Right to Cybersecurity in EU Law? The Challenges Ahead' (2024), Computer Law & Security Review.

Rajesh Kumar and others, 'What Changed in the Cyber-Security after COVID-19?' (2022) 120 Computers & Security 102821.

Roxana Vatanparast, 'Designed to Serve Mankind? The Politics of the GDPR as a Global Standard and the Limits of Privacy', 80(4) Heidelberg Journal of International Law 819-845 (2020).

Simone Boccaletti and others, 'European SMEs' Growth: The Role of Market-Based Finance and Public Financial Support' [2024] Small Business Economics

Sofia Terzi and Ioannis Stamelos, 'Architectural Solutions for Improving Transparency, Data Quality, and Security in eHealth Systems by Designing and Adding Blockchain Modules, While Maintaining Interoperability: The eHDSI Network Case' (2024) 14 Health and Technology 451.

Srinivasan Nagaraj, GSVP Raju and V Srinadth, 'Data Encryption and Authetication Using Public Key Approach' (2015) 48 Procedia Computer Science 126.

Sunil Chaudhary, Vasileios Gkioulos, David Goodman, Cybersecurity Awareness for Small and Medium-Sized Enterprises (SMEs): Availability and Scope of Free and Inexpensive Awareness Resources, Computer Security. ESORICS 2022 International Workshops: CyberICPS 2022, SECPRE 2022, SPOSE 2022, CPS4CIP 2022, CDT&SECOMANE 2022, EIS 2022, and SecAssure 2022, Copenhagen, Denmark, September 26–30, 2022, Revised Selected Papers, vol 13785 (Springer International Publishing 2023).

Vagelis Papakonstantinou, 'Cybersecurity as Praxis and as a State: The EU Law Path towards Acknowledgement of a New Right to Cybersecurity?' (2022) 44 Computer Law & Security Review 105653.

Valentin Mulder and others (eds), Trends in Data Protection and Encryption Technologies (Springer Nature Switzerland 2023).

Vasiliki Tzavara and Savvas Vassiliadis, 'Tracing the Evolution of Cyber Resilience: A Historical and Conceptual Review' (2024) 23 International Journal of Information Security 1695.

Yuanjian Li and others, 'An Efficient Encryption Method for Smart Grid Data Based on Improved CBC Mode' (2023) 35 Journal of King Saud University - Computer and Information Sciences 10174

THESES

Angeliki Barmpetaki, "Data protection: A still developing area in the EU legal order" (LL.M thesis, National and Kapodistrian University of Athens 2023)

WEBSITES

41 Data Privacy Statistics and Facts You Shouldn't Ignore in 2024' (PrivacySavvy) <https://privacysavvy.com/security/safe-browsing/data-privacy-statistics/> accessed 4 September 2024

Alex Hern, 'WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017' The Guardian (30 December 2017) <https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware> accessed 2 September 2024.

APWG - Global Symposium on Cybersecurity Awareness <https://education.apwg.org/safety-messaging-convention/overview/awareness-symposium> accessed 27 September 2024

Big Tech Needs More Regulation' (Meta, 18 February 2020) <https://about.fb.com/news/2020/02/big-tech-needs-more-regulation/> accessed 24 September 2024.

Cecilia Kang, 'OpenAI's Sam Altman Urges A.I. Regulation in Senate Hearing' The New York Times (16 May 2023) <https://www.nytimes.com/2023/05/16/technology/openai-altman-artificial-intelligence-regulation.html> accessed 24 September 2024.

Craig Stuntz - What Is Homomorphic Encryption, and Why Should I Care?' <https://www.craigstuntz.com/posts/2010-03-18-what-is-homomorphic-encryption.html> accessed 25 August 2024.

Cyberspace' (Techopedia, 26 June 2023) <https://www.techopedia.com/definition/2493/cyberspace> accessed 18 September 2024.

Data Protection by Design and Default' (1 July 2023) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and governance/data-protection-by-design-and-default/> accessed 12 September 2024.

Designation of Operators of Essential Services – CSSF' <https://www.cssf.lu/en/2020/10/designation-of-operators-of-essential-services/> accessed 2 September 2024.

ENISA - European Cybersecurity Month <https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/european-cyber-security-month> accessed 27 September 2024.

ENISA - 1st Transport Cyber Security Conference <https://www.enisa.europa.eu/events/first-transport-cyber-security-conference> accessed 27 September 2024.

European DIGITAL SME Alliance, Cybersecurity & Data Protection <https://www.digitalsme.eu/cybersecurity-and-data-protection/> accessed 27 September 2024.

European Maritime Safety Agency, Awareness in Maritime Cybersecurity <https://www.emsa.europa.eu/we-do/safety/maritime-security/item/3477-cybersec.html> accessed 27 September 2024.

GSMA, "The Internet of Things by 2025" <https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf> accessed 23 September 2024.

ISO - ISO/IEC 27000 Family — Information Security Management' (ISO, 25 October 2022) <https://www.iso.org/standard/iso-iec-27000-family> accessed 21 September 2024.

Impact of COVID-19 on Cybersecurity' (Deloitte Switzerland) <https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html> accessed 2 September 2024

Katarzyna Bańkowska, Annalisa Ferrando and Juan Angel García, 'Access to Finance for Small and Medium-Sized Enterprises after the Financial Crisis: Evidence from Survey Data' <https://www.ecb.europa.eu/press/economic-bulletin/articles/2020/html/ecb.ebart202004_02~80dcc6a564.en.html> accessed 27 September 2024.

Microsoft Security Development Lifecycle' <https://www.microsoft.com/en-us/securityengineering/sdl> accessed 14 September 2024.

National Security Alliance, Cybersecurity Awareness Month - National Cybersecurity Alliance <https://staysafeonline.org/programs/cybersecurity-awareness-month/> accessed 27 September 2024.

OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [1980] OECD/LEGAL/0188.

Operational Security - an Overview, ScienceDirect Topics' <https://www.sciencedirect.com/topics/computer-science/operational-security> accessed 21 September 2024.

Report on the Implementation of the OECD Privacy Guidelines' (OECD, 8 November 2023) <https://www.oecd.org/en/publications/2023/11/report-on-the-implementation-of-the-oecd-privacy-guidelines_f13a77a2.html> accessed 26 August 2024.

SentinelOne, 'Cyber Hygiene: 10 Basic Tips For Risk Mitigation' (SentinelOne, 4 December 2018) <https://www.sentinelone.com/blog/practice-these-10-basic-cyber-hygiene-tips-for-risk-mitigation/> accessed 20 September 2024.

The EU Data-Protection Regulation—Compliance Burden or Foundation for Digitization? | McKinsey' <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-eu-data-protection-regulation-compliance-burden-or-foundation-for-digitization> accessed 25 September 2024.

The Revolving Door – from Public Officials to Big Tech Lobbyists | Corporate Europe Observatory' <https://corporateeurope.org/en/2022/09/revolving-door-public-officials-big-tech-lobbyists> accessed 24 September 2024.

The WannaCry Attack Reveals the Risks of a Computerised World' The Economist <https://www.economist.com/leaders/2017/05/20/the-wannacry-attack-reveals-the-risks-of-a-computerised
world?utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=18151738051&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.directresponse.anonymous&gad_source=1&gclid=CjwKCAjwxNW2BhAkEiwA24Cm9Mi1uaLmGIUAgAZfsUaNfDc5JQG2XL0UPSt2zuA1BcI4GqVrMBxYhBoC5GIQAvD_BwE&gclsrc=aw.ds> accessed 2 September 2024.

Tivoli Federated Identity Manager 6.2.2.6' (7 March 2021) <https://www.ibm.com/docs/en/tfim/6.2.2.6?topic=management-policy-tivoli-security-policy-manager> accessed 14 September 2024.

Treaty Revision: Is Europe Ready for a Qualitative Leap?' <https://www.robert-schuman.eu/en/european-issues/725-treaty-revision-is-europe-ready-for-a-qualitative-leap> accessed 23 September 2024.

U.S. Securities and Exchange Commission: The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses <https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html> accessed 27 September 2024.

What Is Application Security?, IBM' (5 June 2024) <https://www.ibm.com/topics/application-security> accessed 21 September 2024.

What Is Data Processing: Cycle, Types, Methods, Steps and Examples | Simplilearn' (Simplilearn.com, 21 October 2020) <https://www.simplilearn.com/what-is-data-processing-article> accessed 7 September 2024.

What Is Front End Development? Comprehensive Guide | Multishoring' (16 April 2024) <https://multishoring.com/blog/what-is-front-end-development/> accessed 13 September 2024.

What Is Personal Data? - European Commission’ <https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en> accessed 4 September 2024.