NIS2: Challenges, Opportunities and Implementation

Francisco Catarino Mendes
Department of Informatics Engineering
University of Coimbra
Coimbra, Portugal
uc2019222823@student.uc.pt

***Abstract*—This paper intends to give an overview of the NIS2 (Network and Information Security) directive, an update of the NIS1 directive. A brief introduction will first be given, which will contain a state-of-the-art regarding the directives and policies used nowadays in the EU concerning cybersecurity, that will be then followed by the discussion section which will contain a definition of the NIS directive, a comparison between NIS1 and NIS2 and a description of the challenges, and opportunities that come along with NIS2, as well as how it can be implemented. Finally, the conclusion summarizes the concepts aborded and sets the stage for what the future holds in this field.**

***Index Terms*—NIS2, Directives, Policies, EU, Cybersecurity**

I. Introduction

In recent times, the European Union has adopted a posture of great responsibility in the cybersecurity world. It has already released many important policies in order to keep strengthening the availability of methods that could help organizations improve their confidence in their cybersecurity implementations and to keep safeguarding communication and data in multiple fields, including politics, energy, economy, healthcare, and the financial sectors, as these have become increasingly dependent on digital technologies [1]. Eventually, all sectors will get to this point, so the EU needs to keep on alert and continue providing help to all sectors of society in the form of new directives and guidelines. With that said, here are the most notable efforts of the European Union regarding the promotion and enforcement of cybersecurity:

ENISA – the EU cybersecurity agency - ENISA (European Union Agency for Cybersecurity) is the EU agency regarding cybersecurity matters. It provides support to Member States, EU institutions, and businesses in key areas [2].

With the appearance of the EU Cyber Security Act, which grants a permanent mandate to the agency, and gives it more resources and new tasks, ENISA now has many new responsibilities, like creating and outlining best practices for cybersecurity, promoting cyber resilience, increasing operational cooperation to help EU Member States better handle relevant incidents, and helping coordinate the EU in case of major cross-border cyberattacks or cybersecurity critical events [1]. It also has a key role in setting up and maintaining the European cybersecurity certification framework by preparing the technical ground for specific certification schemes.

The Cyber Security Act - strengthens the EU Agency for cybersecurity (ENISA) and establishes a cybersecurity certification framework for products and services [5].

Companies doing business in the EU will benefit from having to certify their ICT products, processes, and services only once and see their certificates recognized across the European Union. Furthermore, recently in April 2023, the Commission proposed a targeted amendment to the EU Cyber Security Act, which aims to enable the adoption of European cybersecurity certification schemes for 'managed security services'. These services play an increasingly important role in the prevention and mitigation of cybersecurity incidents [5].

EU Cybersecurity Strategy - was presented at the end of 2020 by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, mainly due to the COVID-19 crisis, which expanded the threat landscape and brought new challenges that required adaptative and innovative responses, therefore making the EU feel like it should be driving norms for solutions and standards of cybersecurity for essential services and critical infrastructures [3].

It covers the security of essential services such as hospitals and energy grids, while also worrying about the security of the number of connected machines present in our homes and in the overall industry, which is a number that will probably not stop growing in the near future, as more and more sophisticated objects keep on being developed [2].

The Strategy focuses on creating the ability to respond to major cyberattacks and outlines how a strong cyber unit can ensure the most effective response to cyber threats using the collective resources and expertise available to the EU and Member States. Also must be mentioned that

the EU is committed to supporting this strategy through an unprecedented level of investment over the next seven years [2], [3].

The Cyber Resilience Act - proposal for a regulation on cybersecurity requirements for products with digital elements, so as to ensure more secure hardware and software products [2].

The two main goals of this Act are to create conditions for the development of secure products with digital elements by ensuring that hardware and software products are made available to their audience with fewer vulnerabilities and ensuring that manufacturers take security seriously as the product is being developed, and to create conditions that allow users to take cybersecurity into account when selecting digital/smart products for purchase [4].

The Cyber Solidarity Act - aims to improve the preparedness, detection, and response to cybersecurity incidents across the EU. It is composed of a European Cybersecurity Alert System (European Cybersecurity Shield), made of interconnected Security Operation Centres, and a complex Cybersecurity Emergency Mechanism to improve the EU's cyber resilience. Besides, the Act establishes a Cybersecurity Incident Review Mechanism to assess and review specific requested cybersecurity incidents [6].

Regarding the European Cybersecurity Shield, it is arranged in national and cross-border Security Operations Centres (SOCs) across the EU, which will use tools such as Artificial Intelligence (AI) and data analytics to detect and communicate warnings on threats to authorities across borders. As for the Cyber Emergency Mechanism, it works in three main principles: testing companies in critical industries such as finance, energy, and healthcare for potential weaknesses that could make them vulnerable to cyberattacks; using the EU Cybersecurity Reserve at the request of Member States or Union Institutions, which triggers incident response services from private service providers; ensuring support to a Member State that offers mutual assistance to another Member State affected by a cybersecurity incident [6].

GDPR - short for General Data Protection Regulation, imposes obligations onto organizations anywhere, as long as they target or collect data related to people in the EU. Concerning penalties, the fines for violating the GDPR are placed in two tiers, which max out at €20 million or 4% of global revenue (whichever is higher). In addition, victims have the right to seek compensation for damages [7].

This regulation is extremely strict, with very detailed nuances in data protection principles, accountability, data security, data protection by design, consent from data subjects, and people's privacy rights, among others. Data Protection Officers are also relevant, which are professionals whose basic tasks involve understanding the GDPR and how it applies to the organization, advising people in the organization about their responsibilities, monitoring GDPR compliance, and others.

As one can see, GDPR is of incredible help when talking about confidentiality issues. By adhering to GDPR rules, it is very probable that a company is treating its data in a secure way which leads to the chances of a data leak plummeting.

Digital Operational Resilience Act - also known as DORA, entered into force on 16 January 2023 and will apply as of 17 January 2025. Aims at making the IT security of financial entities the best it can be and making sure that the financial sector in Europe is able to stay operational may it suffer a major disruption [8].

This Act covers ICT risk management, ICT third-party risk management and oversight of third-party providers, because of the importance of having a secure supply chain nowadays, digital operational resilience testing, reporting of ICT-related security problems, and information sharing [8].

And, of course, there is also the **NIS2 Directive**, the main topic of this paper, which will be described in more detail in the Discussion section. As one can verify, the European Union has made great progress in reaching the objective of providing its Member States the ability to have the best cybersecurity practices and recommendations in place. However, going forward the EU also has to keep in mind that these regulations and policies greatly impact institutions performance-wise, so the strictness level and the amount of regulations that come out must not be overwhelming to the point that organizations begin to dread the cybersecurity topic.

The remainder of the paper contains information on the NIS Directive, from the reasons that led to the update of NIS to NIS2, to the challenges, opportunities, and implementation methods it brought along.

II. Discussion

A. What is the NIS directive?

The Directive on Measures for a high common level of cybersecurity across the Union, most known as NIS, is the EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU [9].

Since this is a directive and not a regulation, it does not automatically apply in all EU countries but first must be converted into national law by all EU Member States.

NIS ensures Member States' preparedness, by requiring them to be appropriately equipped. A Computer Security Incident Response Team (CSIRT), which is responsible for

risk and incident handling, a national network and information systems (NIS) authority, and a single point of contact (SPOC) are normally considered the best composition of resources.

It also provides cooperation among all the Member States, with the set up of a Cooperation Group to make it easier and support strategic cooperation and intelligence communication among Member States.

Moreover, the Directive creates a culture of security across seven sectors that are vital for our economy and society and that rely heavily on ICTs, such as energy, transport, banking, financial market infrastructures, drinking water, healthcare, and digital infrastructure [9]. Once again, this is a very important aspect, as these sectors will be dependent on the digital space to perform their duties and to establish connections with each other.

Corporations identified by the Member States as operators of essential services in the above sectors have to take the security actions needed so that their processes are at the minimum risk of being exploited, using the resources the EU has provided, among others as well, and must notify relevant national authorities in the case of concerning incidents. On another note, digital service providers, like cloud computing services, also must comply with the requirements the Directive presents [9].

But despite the Directives' notable achievements in the security of network and information systems, which led the way for a significant change in the mindset and approaches that many Member States had regarding cybersecurity, NIS ended up with its limitations being found out.

B. From NIS to NIS2 - Why was it updated?

As time passed by, when reviewing NIS, the main findings were that the scope of the NIS directive is too limited in terms of the sectors covered, and also presented some other weaknesses [10]:

- Ambiguous rules and insufficient coordination between Member States;
- Inadequate level of cyber resilience of companies and Member States resulting from a lack of common understanding of the primary threats;
- Some vital sectors remained outside the scope;
- Insufficient exchange of information between Member States;
- Lack of a well-built crisis preparedness;
- Increased digitalization and a need for a higher degree of interconnectedness;
- Weak enforcement.

COVID-19 also helped in making the NIS directive subject to a dire need of an update, as most of the population had to resort to the online world for working and daily basis purposes. The threat scenario grew and brought numerous new challenges, which required innovative responses. In recent times, any disruption, even one initially confined to one entity or one sector, can have a snowball effect propagated into other areas, potentially resulting in far-reaching and long-lasting negative impacts on the delivery of services across the whole internal market [11].

C. NIS2 - Changes

The key change that needs to start this section off is the new and expanded scope of the Directive. New sectors were added based on their criticality for the economy and society. A size cap was also introduced so that all medium and large companies in selected sectors can be included in the scope, while at the same time leaving some flexibility for Member States to identify smaller entities with higher cybersecurity risk profiles, which would naturally need some attention [11].

The NIS2 directive expanded coverage from the original 7 sectors under the NIS directive and added 8 more for a total of 15 sectors, with 8 characterizing as "Essential Entities" and 7 as "Important Entities" [12]. The sectors can be visualized in Figures 1 and 2 below:

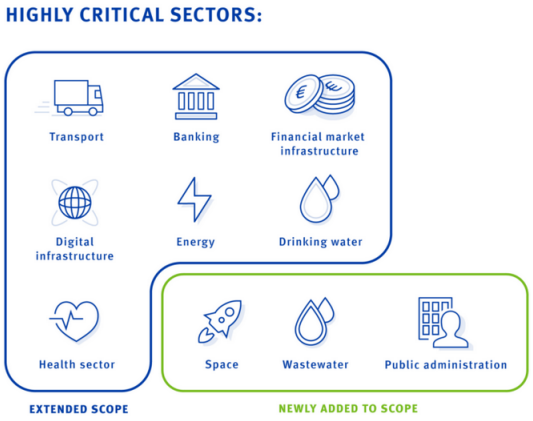

Figure 1: Highly Critical Sectors [13]

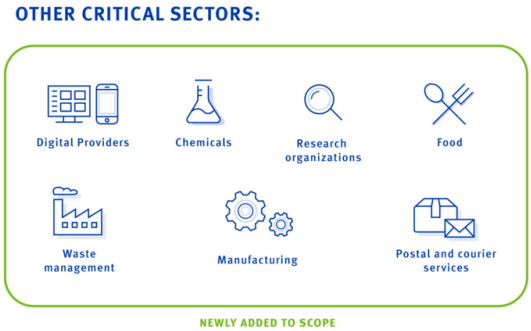

Figure 2: Other Critical Sectors [13]

Basically, what the NIS2 Directive ended up deciding was to group ”Drinking Water” and ”Waste Water” into only one sector, named ”Water Supply”, and also group ”Banking” and ”Financial Market Infrastructure” into just the ”Finance”, sector. This way, the counting of 15 sectors is confirmed. Finally, Figure 3 displays which are the ”Essential Entities” and the ”Important Entities”:

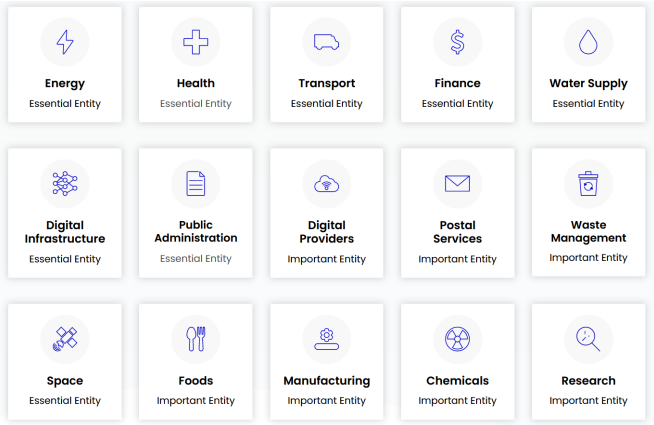

Figure 3: Essential and Important Entities, categorized [12]

Moving on to the aspect of the size of a company, NIS2 defines said factor following the rules below [13]:

- **Large Company -** employs at least 250 people or has annual sales of more than 50 million euros, or total assets of more than 43 million euros;
- **Medium-Sized Company -** has between 50 and 249 employees or generates annual sales of up to 50 million euros, or total assets of between 10 and 43 million euros;
- **Small Company -** employs fewer than 50 people or has annual sales or total assets of up to 10 million euros. Not all of them fall under NIS2 requirements.

The Directive does not even take into consideration the size of the organization if it falls under any of these categories: providers of public electronic communications networks or publicly available electronic communications services; providers of trust services; Top-level domain registrars and DNS service providers; providers acting as the sole provider of a service in a Member State and whose service is essential for the maintenance of critical social or economic activities; providers where disruption of its services could have a significant impact on public order, public security, or public health. All of these entities are automatically under the NIS2 Directive [13].

Moving on, NIS2 also targets strengthening security requirements for the companies by introducing new requirements and obligations for organizations in four interconnected areas:

Risk Management - now, enterprises must take measures to minimize cyber risks. These measures include [14]:

- Risk assessments and security policies for information systems;
- Policies and procedures for the use of cryptography;
- Possessing policies for handling and reporting vulnerabilities;
- Security procedures for employees with access to sensitive or important data, as ethical-based situations can occur;
- The use of multi-factor authentication and other authentication mechanisms;
- Policies and procedures for evaluating the effectiveness of security measures;
- A plan for handling security incidents;
- Cybersecurity training and sensibilization;
- A plan for managing business operations during and after a security incident;
- Security around supply chains. This will drive a much-needed change in the mindsets of organizations when it comes to cyber risk management. Most security professionals say their organizations are at risk because of their inability to verify the security practices of relevant third parties and mitigate cyber risks across the external supply chain [15].

Corporate Accountability - NIS2 requires corporate management to oversee, approve, and be trained on the entity’s cybersecurity measures and to address cyber risks. Failing to do so can result in penalties for management, including liability and a potential temporary ban from management roles.

Reporting Obligations - essential and important entities must have processes in place for the immediate reporting of security incidents with significant impact on their service processes. NIS2 sets specific notification deadlines, such as a 24-hour “early warning”.

Business Continuity - enterprises must plan for how they intend to ensure business continuity in the case of major cyber catastrophes. This plan should include considerations about system recovery, emergency procedures, and setting up a crisis response team.

The NIS2 Directive also gives more weight to the role of the NIS Cooperation Group in shaping strategic policy decisions on emerging technologies and increases information sharing and cooperation between Member State authorities [11].

Finally, penalties and fines for NIS2 violations were also adjusted and became more strict. Non-compliance can result in non-monetary penalties, administrative fines, or criminal sanctions. Non-compliance examples are infractions such as

failure to meet security requirements and failure to report incidents. The specific fines will vary depending on the Member State, but the Directive establishes a minimum list of administrative sanctions [16]. Concerning the details of the fines, those are shown next, inside of the respective categories:

Non-monetary Penalties - are composed of compliance orders, binding instructions, security audit implementation orders, and threat notification orders to entities' customers.

Administrative Fines - vary between Essential and Important Entities. For Essential Entities, NIS2 requires Member States to provide a maximum fine level of at least €10,000,000 or 2% of the global annual revenue, whichever is higher. As for Important Entities, the Directive requires Member States to fine for a maximum of at least €7,000,000 or 1,4% of the global annual revenue, whichever is higher.

Criminal Sanctions For Management - these are sanctions that hold top management personally liable and responsible for proven gross negligence in the event of a security incident, to attempt to lower the pressure put on IT departments to ensure the security of the organization only by themselves. Every member of an institution must be aware of the cybersecurity challenges his company faces, starting from the top. Therefore, penalties can be having to make compliance violations public, making public statements identifying the natural and legal person(s) responsible for the violation and its nature, or temporarily banning an individual from holding management positions in case of repeated violations, if the targeted company classifies as an Essential Entity.

And with all of this information written and exposed, the NIS2 changes are finally over. Overall, these constitute great progress in making sure that all Member States are as ready as possible to help their organizations prepare and react in the best way possible to cyber attacks. As it is widely known, it is impossible to be 100% safe and secure, so entities must aim to be as secure as they can be, utilizing all the tools at their disposal.

D. NIS2 - Challenges

With all of these changes, naturally, NIS2 brings some challenges to the Member States and to every industry Entity that is going to be under the Directives' legislation.

For starters, NIS2 is extremely strict. As one can see from the list of requirement measures, they constitute a considerable number, and some might be hard for companies to implement. The effort these Entities will have to make in order to successfully pass all the requests will be much higher than before. Penalties are also much heavier now, and if an organization is caught slacking, it will suffer consequences that can have a considerable impact on its functionality. The penalties can even come from reasons totally not related to the desire to have a robust cybersecurity component, as enterprises must, before anything else, know if this legislation applies to them or not. Being oblivious is a huge problem, so the right professionals need to be employed, and the management must be composed of educated individuals.

Then, reporting obligations exist when an Entity is victim of a successful cyber attack. An Essential Entity aware of the occurrence of a significant cybersecurity incident must provide an early warning without undue delay, and at the latest within 24 hours, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or if it could have a cross-border impact. The early warning should be followed by an incident notification to the competent authorities within 72 hours containing an assessment of the incident, the severity, impact, and indicators of compromise. A final report is then to be submitted within 1 month of the incident notification by the national CSIRT or competent authority. The Member States should ensure that the notification requirement does not divert resources from activities related to incident handling [15]. All of this can be overwhelming for a company to go through, when at the same time, incident recovery processes are underway and everybody is under much stress.

The increased impact of the NIS2 Directive is also a challenge. The interconnections and the exchange of information faced huge growth, as more sectors were added to the scope. Figure 4 shows what was the expected impact on the EU, in 2023 [17]:

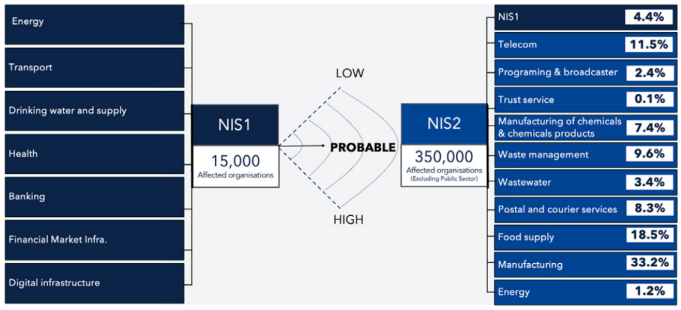

Figure 4: Extended Impact of NIS2 on the EU in 2023 [17]

The analysis is partly based on a calculation of how many medium and large-sized organizations are in the affected sectors, as well as an estimate of organizations needing to comply with the Directive to be able to supply products or services to the sectors in scope [17].

Finally, implementing the NIS2 Directive comes with new costs, and requires investments. The size of these investments depends on how complex and extensive the workload is for the business and the approach they choose. For existing NIS Entities, who already followed the previous Directive, costs are estimated to be 12% more within the information

security budget, while organizations not previously under the NIS legislation can expect 22% more costs within their information security budget [17].

E. NIS2 - Opportunities

Regarding the opportunities NIS2 brings, for starters, third-party risks must be addressed. According to research conducted by Applied Risk in 2021, only 33% of professionals say their organizations conduct regular audits of their own main suppliers, and only 27% conduct due diligence prior to contracting with new suppliers. Just half (49%) of security professionals say their contracts with suppliers include cybersecurity requirements. Another research conducted by DNV in 2022 reveals that 28% of energy professionals say their company is making the cybersecurity of their supply chain a high priority for investment [15].

Evidently, these percentages are extremely worrisome and low. But with NIS2's new requirements, especially those regarding supply chain cybersecurity matters, organizations now have the opportunity to become safer and more resilient when dealing with third-party incidents.

While some of these might overlap the challenges, if those challenges are indeed overcome, they are transformed into opportunities. For example, as already said NIS2 sets more stringent cybersecurity requirements for essential and important Entities, including measures like risk analysis, incident handling, and business continuity. In fact these rules, if well applied, end up giving organizations the help they need to improve their overall cybersecurity posture.

Furthermore, NIS2 promotes greater sharing of information about cyber threats and vulnerabilities between Entities and with national authorities. This can help organizations respond more effectively to incidents and improve national and EU-wide cybersecurity resilience. Also, the Directive seeks to harmonize cybersecurity practices across all Member States, reducing the differences in cybersecurity readiness. This creates a more level playing field and can facilitate smoother operations for organizations operating in multiple EU countries.

Moreover, the investment that now has to be put into being compliant can eventually lead to advancements in cybersecurity technologies and services, benefiting the economy and the security landscape. Once again, challenges turn into advantages. Finally, as part of the efforts to comply with NIS2, there is an increased focus on training and building cybersecurity skills within organizations, from top to bottom. This not only helps in meeting compliance but also increases the amount of educated professionals in the cybersecurity environment.

F. NIS2 - Implementation

An organization must be methodical when implementing the NIS2 Directive. It must go through 3 steps: knowing from the start which systems are within the scope; adopting risk-based cybersecurity management and enforcing security controls; and documenting everything needed to demonstrate compliance with controls [15]. These steps are described below:

Understanding the scope - first of all, if not in scope, the Entity must know whether its third-party suppliers are, and adjust conformably. Otherwise, the Entity must know what essential services it provides, which requirements would need to be implemented, and what obligations would need to be attributed to its suppliers. Therefore, the main conclusion from the first step is that understanding the scope and the regulatory requirements is important for both organizations directly or not directly impacted by NIS2.

Risk-based cybersecurity management systems - this part is straightforward. Essential and Important Entities within the scope of NIS2 will be required to take appropriate technical, operational, and organizational measures to manage the risks posed to the security of their operations and services. Besides, the new requirements and obligations the Directive sets must be implemented at this phase.

Documentation for demonstration - after all the technical procedures are in place, compliance requires documentation, because, without proof, nothing can be guaranteed. Auditors can ask for a wide range of documentation in assessing organizations for verifying compliance with NIS2, so Entities must be ready and be in possession of the proper paperwork.

This was a brief description of the procedure, but by following these steps, organizations can rest assured that they will be compliant with the NIS2 Directive, and so will have a high chance to prosper, free of cybersecurity incidents. Re-evaluation is, of course, needed, as time passes by.

III. Conclusion

With this paper, a lot was learned about the new NIS2 Directive. Before diving into its components, a brief introduction was made talking about the EU's efforts to improve the cybersecurity scenario. Regarding NIS2, its overall definition and purpose were given, followed by the reasons it was updated from its previous form. Then, the changes it was subject to were narrated and exposed, going from the new scope to the heavier penalties. Finally, its challenges and opportunities were presented, along with the main steps that an organization should follow to successfully implement the Directive.

Limitations to this assignment could be the lack of information on some parts, mainly the opportunities and the implementation sections, and the lack of a real-life example

in a specific industry, such as energy for example. Future work can be done regarding the missing information and details that may exist but were not shown here, and related to what the future holds for this Directive, as it will probably keep on being updated as technology and the cybersecurity landscape keeps on evolving.

REFERENCES

[1] Sen, K.: ”List of Cybersecurity Regulations in the European Union”, available at https://www.upguard.com/blog/cybersecurity-regulations-in-the-european-union. August 25, 2023.

[2] European Commission: ”Cybersecurity Policies”, available at https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies.

[3] European Commission: ”The Cybersecurity Strategy”, available at https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

[4] European Commission: ”Cyber Resilience Act”, available at https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act. September 15, 2022.

[5] European Commission: ”The EU Cybersecurity Act”, available at https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.

[6] European Commission: ”The EU Cyber Solidarity Act”, available at https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity.

[7] Wolford, B.: ”What is GDPR, the EU’s new data protection law?”, available at https://gdpr.eu/what-is-gdpr/.

[8] EIOPA: ”Digital Operational Resilience Act (DORA)”, available at https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en.

[9] European Commission: ”Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)”, available at https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

[10] Byttebier, P.: ”NIS-2: Revolution or solid ground for security?”, available at https://blog.cybersecuritycoalition.be/wp-content/uploads/Pieter-Byttebier-NIS2.pdf.

[11] European Commission: ”Proposal for directive on measures for high common level of cybersecurity across the Union”, available at https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union.

[12] NIS2 Directive: ”The NIS2 Directive Explained”, available at https://nis2directive.eu/.

[13] Hiess, M.: ”NIS2 directive brings major challenges”, available at https://anexia.com/blog/en/nis2-directive-brings-major-challenges/. July 28, 2023.

[14] NIS2 Directive: ”NIS2 Requirements”, available at https://nis2directive.eu/nis2-requirements/.

[15] DNV: ”NIS2 DIRECTIVE”, available at https://brandcentral.dnv.com/original/gallery/10651/files/original/5a2853da-dd83-4fa1-8071-253d93767198.pdf.

[16] NIS2 Directive: ”NIS2 Fines”, available at https://nis2directive.eu/nis2-fines/.

[17] CISCO Public: ”Transforming NIS2 Challenges into Strategic Opportunities”, available at https://www.cisco.com/c/dam/global/EMEAR_Security/EU_NIS2_white_paper_080124.pdf.