

THE EVER-INCREASING CYBERSECURITY COMPLIANCE IN EUROPE: THE NIS 2 AND WHAT ALL BUSINESSES IN THE EU SHOULD BE AWARE OF

VALENTINO LUCINI,

PhD Candidate

Sun Yat-sen University, Guangzhou (China)

Abstract: On 27 December 2022, the Network and Information Systems (NIS) Directive 2 has been published on the Official Gazette of the European Union and became effective 21 days after. The NIS 2 represents the new attempt by the Union to create a more solid regional cybersecurity legal framework and requirements after the fragmented adoption of the previous NIS Directive by its Member States and gives the latter until 17 October 2024 to adapt their legislations. The new directive widens the reach of the previous discipline by including more enterprises in the scope of application as well as new sectors. Further, the Union is lifting the burden of classification from the Member States by replacing it with an identification based on company's dimension. But that's not all. The NIS 2 revises also most of cybersecurity requirements of the previous discipline by providing a list of new obligations as well as revised procedural terms and liabilities. In this context, many operators previously exempt by the NIS Directive could now face new compliance challenges when operating in Europe whereas companies already subject to NIS 1, should also reassess their stance in order to limit their legal risks in the region. The article provides an outline of the new reach of the NIS 2 Directive, its main provisions and provides suggestions for EU and foreign operators (including Russians) in order to be prepared for the changes the NIS 2 regulatory system would bring.

Keywords: NIS 2 · Network and Information Systems (NIS) Directive · Directive (EU) 2016/1148 · Directive (EU) 2022/2555 · foreign companies in Europe · EU cybersecurity

1. Introduction

On 28 November 2022 the Network and Information Systems (NIS) Directive 2 was approved by the European Council¹ following the Parliament approval few weeks before². On 27 December, it was published on the Official Gazette European Union³, and Member States would have until 17 October 2024 to adapt their national legislation to the new rules. This represents the normative answer enacted by the European Union (EU) to counter the increasing number of cybersecurity incidents and finally push a real common cybersecurity framework agenda to entities, both public and private, in specific sectors and within precise dimension. The NIS 2 follows the European Commission discourse to update the EU's cybersecurity legislation in its Cybersecurity Strategy

¹ Council of the European Union, "EU Decides to Strengthen Cybersecurity and Resilience Across the Union: Council Adopts New Legislation," news release, December 1, 2022, accessed December 1, 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/?utm_source=dsms-auto&utm_medium=email&utm_campaign=EU+decides+to+strengthen+cybersecurity+and+resilience+across+the+Union%3a+Council+adopts+new+legislation.

² European Parliament, "Cybersecurity: Parliament Adopts New Law to Strengthen EU-Wide Resilience," news release, December 1, 2022, accessed December 1, 2022, <https://www.europarl.europa.eu/news/en/press-room/20221107IPR49608/cybersecurity-parliament-adopts-new-law-to-strengthen-eu-wide-resilience>.

³ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measure 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), 65 (27 December 2022), accessed January 1, 2023, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555&from=IT>.

considering the economy's increased reliance on technology and the Covid-19 pandemic.⁴ However, this request for revision came just after few years from the first Network and Information Systems (NIS 1), which was enacted via the Directive (EU) 2016/1148 of 6 July 2016, also aimed at the same scope: achieve common level of cybersecurity across the region.⁵

The Member States had more than two years (i.e., until November 9th, 2018)⁶ to identify entities subject to the NIS 1, called operators of essential services (OES)⁷. Nevertheless, after the Commission was called to evaluate the NIS 1 performance, it discovered several issues.⁸ For example, not all industries expected to fall under this cybersecurity framework were covered by NIS 1, the discipline provided too much latitude in deciding what sorts of cybersecurity and incident reporting standards to impose on OES, and NIS 1 lacked effective enforcement and supervision in the implementation.⁹ For those and other reasons, the Commission proposed to replace the NIS 1 with NIS 2 which would increase the reach of application to cover more entities in existing sectors of the discipline as well as include new fields left out in the previous directive.¹⁰ This would be achieved by the replacement of the previous classification of essential services and digital service providers with sector agnostic categories of important and essential entities. Further, the Union is lifting the burden of classification from the Member States by replacing it with an identification based on company's dimension.¹¹

Because of the greater reach of the NIS 2 discipline, more entities would be subject to the European cybersecurity discipline in the coming future whereas companies already subject to the previous rules shall re-assess their position to new requirements. It may appear to be a long way to go until Member States would have completed their implantation (i.e., October 2024). However, given the level of detail involved in the NIS2 Directive's obligations and the timeline for implementing the directive's measures, companies must implement internal safeguards, both technical and organizational, as soon as possible so to protect themselves from potential cyber-attacks and to be ready for the stringent requirements that the NIS 2 Directive will impose on relevant sectors. For those reasons, this article aims to shed some light on the impact to entities operating in Europe would face by firstly addressing the enlarged scope of application of the NIS 2 and later by tackling the most concerning new requirements. Finally, the article will introduce some suggestions to be taken beforehand and penalties in case of failure to comply with the new rules.

2. The NIS 2 scope of application

The NIS 2 is not a simple revision of the previous discipline but contains many important differences that aim to achieve a better degree of harmonization with regard to security standards

⁴ "Joint Communication to the European Parliament and the Council—The EU's Cybersecurity Strategy for the Digital Decade" JOIN (2020) 18 final (European Commission, 2020).

⁵ 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.

⁶ Article 25 Paragraph 1 and Article 5 Paragraph 1 of NIS 1,

⁷ The drafter of the NIS 1 chose the name "operators of essential services" because those entities provide services which were essential for the maintenance of critical societal and/or economic activities.

⁸ "Commission Staff Working Document Impact Assessment Report Accompanying the Document 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" SWD/2020/345 final (European Commission, 2020), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0345>.

⁹ Ibid., Annex 5 page 81.

¹⁰ European Commission, *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* (2020), COM/2020/823 final, accessed November 26, 2022, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN>.

¹¹ S. Schmitz-Berndt, "European Union · Cybersecurity Is Gaining Momentum - NIS 2.0 Is on Its Way," *European Data Protection Law Review* 7, no. 4 (2021), doi:10.21552/edpl/2021/4/14, <https://edpl.lexxion.eu/article/EDPL/2021/4/14>.

and reporting duties in the Union.¹² Arguably, among the most important changes there is the replacement the complex identification process in the hand of the Member States as established in Article 5 of the NIS 1 with a self-identification system based on sectors and dimension of the entity. In this sense, the Article 2 Paragraph 1 of the NIS 2 applies to public and private entities which qualify as medium-sized enterprise or above and belonging to the category of essential entities as per Annex I and important entities as per Annex II, with the exclusion of micro and small enterprises.¹³ This means that entities not falling in the sectors listed in the annexes or even falling within it but having less than 50 workers and an annual balance sheet of less than EUR 10 million¹⁴, shall be excluded from the application of the normative. Consequently, the new “size-cap rule” shifts the burden of identify the scope of application of NIS from State Members - with the old system of national competent authority determination¹⁵ - to the entities themselves. Further, the NIS 2 identifies certain types of entities under special regime for which the size-cap does not apply and are subject to the NIS 2 regardless of the dimension.¹⁶

The second novelty brought by the NIS 2 is the replacement of the NIS 1 categories of operators of essential services (OES) and digital service providers (DSP) with technology agnostic categories of “essential entities” and “important entities”.¹⁷ In this way, entities falling within a certain sector listed in the Directive and its annex are assigned to that category. In addition, the sectors provided in NIS 1 are further expanded including advanced and strategic technologies, as can be seen from Table 1 below.

Table 1 Comparison of sectors in NIS 1 and in NIS 2.

Sectors of High Criticality		Other Critical Sectors	
NIS 1	NIS 2	NIS 1	NIS 2
Energy: electricity; oil and gas	Added production; aggregation; demand response and energy storage; electricity markets; district heating; and hydrogen	Digital providers: online marketplaces; online search engines	Added social networking services
Transport (air; rail; water; road)	Same	-	Added waste management
Banking	Same	-	Added manufacture, production, and distribution of chemicals:
Financial market infrastructures	Same	-	Added food: production; processing; and distribution.
Health: healthcare	Added EU reference labs; research and manufacturing of	-	Added manufacturing: medical devices; computer,

¹² Andreas Gruber and Natalie Ségur-Cabanac, “Necessary or Premature? The NIS 2 Directive from the Perspective of the Telecommunications Sector,” *International Cybersecurity Law Review* 2, no. 2 (2021), doi:10.1365/s43439-021-00035-6, <https://link.springer.com/article/10.1365/s43439-021-00035-6>.

¹³ Article 2 Paragraph 1 of the NIS 2.

¹⁴ See the Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

¹⁵ Article 8 Paragraph 1 of the NIS 1.

¹⁶ Article 2 Paragraph 2, 3 and 4 of the NIS 2.

¹⁷ Article 3 of the NIS 2.



	pharmaceuticals and medical devices		electronic and optical products; electrical equipment; machinery; motor vehicles and trailers and semi-trailers; and transport equipment.
Drinking water	Same	-	Added postal and courier services
Digital infrastructure: Internet Exchange Point providers; DNS; TLD name registers; cloud computing; content delivery network providers; trust service providers;	Added data centre service providers; and Electronic communications		Added Research sector
-	Added waste water		
-	Added Public administrations		
-	Added Space		
-	ICT-service management (B2B): Managed service providers (MSP); Managed Security service providers (MSSP)		

It shall be noted the NIS 2 also specifies that some companies will be exempt from its scope. This comprises public administration institutions engaged in activities such as defense, national security, public security, or law enforcement.¹⁸

The above list is based on a territorial scope of application because it applies to entities under the jurisdiction of the Member State in which they are established.¹⁹ However, entities in the following sectors are subject to special jurisdiction (Table 2)²⁰:

Table 2 Special Jurisdictions

Sector	Jurisdiction
Providers of public electronic communications networks or providers of electronic communications services (Annex I point 8).	Member State in which they provide their services
DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery	Member State in which they have their main establishment in the Union

¹⁸ Article 2 Paragraph 7 of the NIS 2.

¹⁹ Article 26 Paragraph 1 of the NIS 2

²⁰ See Recital (64) and Article 24 of the NIS 2.



network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines or of social networking services platforms.

Public administration entities.

Member State which established them

Further, the NIS provides also for an extraterritorial reach by requiring certain entities not established in the Union but offering services within it, to designate a representative in the Union. This is the case of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines or of social networking services platforms that are not established in the Union.²¹

Entities subject to the NIS 2 will be required to provide specific information to the relevant authorities in connection with the Member States' list of essential and important entities and the European Union Agency for Cybersecurity (ENISA) registration of essential and important entities.²² Member States may adopt national processes requiring entities to register in order to establish and update the list.

3. Impact on business operators in the EU: new risk management requirements and reporting

The addition of new sectors to NIS2, along with the size-cap regulation, should result in a dramatic increase in the number of organizations covered by the directive. Even though at the current stage it is difficult to predict the exact digit, it is expected to be seven times greater than before, bringing the estimated 15,500 current OES under the old the NIS 1 up to roughly 110,000 entities subject to NIS 2.²³ But this impact could be even bigger. While the reference to types of entities in Article 2 paragraph 2 do not generally create problems, the criteria for the classification are more concerning and could potentially result in the inclusion of providers with only few employees and an annual turnover below 10 million.²⁴ Further, in some sectors the definition adopted by the Union seems to be overreaching and, sometimes, going even further than what is currently established by Member States.²⁵

The increasing reach of NIS 2 and uncertainties related to the interpretation of certain criteria, couple with broad definition of certain sector would probably translate into an increase of number of entities subject to the new discipline and related requirements. For example, the automotive sector is now listed in the NIS Annex II as Other Critical Sector, and consequently, will requires entities in this field with presence in Europe to abide by the new requirements. This means that, for example, the China's top electric car manufacturer and second-largest battery manufacturer BYD would be subject to the NIS 2 in case it decides to produce their vehicles or part of them in the EU.²⁶ The same would apply to Russian manufactures like AvtoVAZ, GAZ, etc.

Also the health sector is expanded to include EU reference labs; research and manufacturing of pharmaceuticals and medical devices, which were particularly critical during the Covid-19

²¹ See Recital (34) and Article 26 Paragraph 3.

²² Article 3 Paragraph 3 and 4.

²³ European Commission, "Commission Staff Working Document Impact Assessment Report Accompanying the document 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," Page 20.

²⁴ Thomas Sievers, "Proposal for a NIS Directive 2.0: Companies Covered by the Extended Scope of Application and Their Obligations," *International Cybersecurity Law Review* 2, no. 2 (2021): Page 226, doi:10.1365/s43439-021-00033-8, <https://link.springer.com/article/10.1365/s43439-021-00033-8>.

²⁵ Ibid.

²⁶ Investor's B. Daily, "Nio, BYD, China EV Makers Make Historic Push into Europe," *Investor's Business Daily*, September 30, 2022, accessed November 27, 2022.

pandemic.²⁷ Hence, investments in this field will also bring new cybersecurity requirements as provided by NIS 2.²⁸

It shall be noted that the NIS 2 does not apply only to new investments but instead to all entities operating in specific fields provided by the Annex I and Annex II, and that possess the dimensional requirements, unless exceptions apply. For this reason, historical business operators in Europe would also need to readdress their position considering the implementation of this legislation. For example, among the essential service as per Annex I of the NIS 2, we now count the digital infrastructure, which include also data centre service providers.²⁹

From the above, it is highly foreseeable that the NIS 2 will have a major impact on more business operator in Europe compared to the previous discipline, due it territorial and extraterritorial reach. Nevertheless, one could wonder what the new Directive requirements are and whether companies belonging to one category would have different cybersecurity compliance obligation than the others. To answer the latter, the NIS 2 make it clear in various passages that entities in both categories—important entities and essential entities—must meet the same cybersecurity and reporting criteria.³⁰ This means that, no matter the sector involved, entities shall all “take appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimize the impact of incidents on recipients of their services and on other services”.³¹ Those measures should guarantee a degree of security of network and information systems proportionate to the risk presented, taking into account the “state of the art” and, if applicable, relevant European and international standards, as well as the cost of implementation.³² When examining the proportionality of such measures, the degree of the entity's exposure to risks, its size, the possibility of occurrence of accidents and their severity, including their societal and economic impact, must all be considered.³³

Another novelty of the NIS 2 is about the new regime of corporate governance, responsibility, and accountability of management bodies for the compliance with cybersecurity requirements. Article 20 of the NIS 2 stipulates that Member States should take all steps to ensure that the management bodies of essential and important entities approve the measures adopted by such organizations, oversee their implementation, and are accountable in case of failure.

To guarantee that management bodies do follow through with the implementation of the new requirements and those are clearly understood by the officer, the NIS 2 requires training to them as well as suggest that such training activities would be extended to all employees on a regular basis.³⁴

In case entities subject to NIS 2 discipline would be worried about compliance standards and how to demonstrate accountability, it shall be said that the Directive provides some assistance. It allows Member States to mandate the use of specific ICT products, services, and processes that have received certification under European cybersecurity certification schemes after having complete an impact assessment and stakeholder consultation.³⁵ This also includes products and services offered by third parties, whereas the Commission is empowered to specify which kinds of essential and important entities has to get certification in order to be compliant.³⁶ This means, for example, that

²⁷ Annex I Point 5 to the NIS 1

²⁸ *Reuters Media*, “China's Mindray to Buy Diagnostic Test Material Supplier HyTest for \$661 Mln,” May 17, 2021, accessed November 27, 2022, <https://www.reuters.com/business/healthcare-pharmaceuticals/chinas-mindray-buy-diagnostic-test-material-supplier-hytest-661-mln-2021-05-17/>.

²⁹ Annex I Point 8 to the NIS 2.

³⁰ Article 21 and 23 of the NIS 2.

³¹ Article 21 Paragraph 1 of the NIS 2.

³² *Ibid.*

³³ *Ibid.*

³⁴ Article 20 Paragraph 2 of the NIS 2.

³⁵ Article 24 Paragraph 1 of NIS 2.

³⁶ Article 24 Paragraph 2 of NIS 2.

a foreign social network deployed in Italy could follow the scheme of the Italian *Perimetro di Sicurezza Nazionale Cibernetica*, and purchase ICT products from companies listed therewith and limit potential legal risks.³⁷ For the same token, foreign suppliers of ICT products and services in Europe should follow specific Member State national laws to get certified, so to be allowed to sell their products and services to essential and important entities in the near future.³⁸

Another novelty which would have a critical impact on all business entities operating in Europe is related to the incident management and notification. First of all, all entities should be aware that not all cyber events are the same and, consequently, they should distinguish between an incident and a cyber threat in the context of reporting. In case of an incident having a significant impact on the delivery of services³⁹, the entity shall submit a report to the Computer Security Incident Response Teams (CSIRT) or to the competent authority (if relevant) within the following timeframe⁴⁰:

- a) an early warning without undue delay and, in any case, within 24 hours after learning about the occurrence of the event;
- b) incident notice without undue delay and, in any case, within 72 hours of becoming aware of the incident;
- c) an interim report upon request from a CSIRT or the competent authorities;
- d) a final report that must be submitted no later than one month after point b).

Entities would be required to provide a “progress report” at the time of the final report submission in circumstances where incidents were still ongoing, and a final report within a month following the incident's resolution. When applicable, such organizations must promptly inform service recipients about situations that are likely to have a negative impact on the delivery of that service.

Regarding significant cyber threat, instead, essential and important entities should immediately notify any actions or remedies that their service receivers may be able to adopt in response to the possible danger. The entities must, if necessary, also inform those receivers of the threat itself.⁴¹

Understanding this difference between incidents and threats is therefore essential to avoid legal pitfall or wasting companies' resources. In fact, while a threat is a probability that a specific type of attack may occur, cyber incidents usually denoted a breach of a system's security policy that is affecting its integrity or availability or confidentiality and/or the unauthorized access or attempted access to a system or systems.⁴² Therefore, misclassifying an event could cause a company to not report an incident because it believes it's just a threat and vice-versa.

4. Suggestions and sanctions.

The above articles showed an increasing reach of the NIS 2 as well as new requirements and notification obligations. Hence, all entities operating in Europe (both local and foreign) or foreign entities interested in the European market should start assessing their position in advance before the NIS 2 will be implemented by Member States in 2027, so as not to be found unprepared. In this section, the article suggests certain measures entities should take in order to limit their legal exposure.

³⁷ On the topic of Italian legislation maturity compared to NIS 2, see Sandra Schmitz-Berndt and Pier G. Chiara, “One Step Ahead: Mapping the Italian and German Cybersecurity Laws Against the Proposal for a NIS2 Directive,” *International Cybersecurity Law Review* 3, no. 2 (2022), doi:10.1365/s43439-022-00058-7.


³⁸ Ibid., Page 301.

³⁹ The Commission shall establish implementing actions with respect to specific kinds of entities that further define the circumstances under which an incident shall be deemed significant.

⁴⁰ See Article 25 Paragraph 4 of NIS 2.

⁴¹ See Article 23 Paragraph 2 of NIS 2.

⁴² *National Cyber Security Centre*, “What Is a Cyber Incident,” Invalid DateTime, accessed November 29, 2022, <https://www.ncsc.gov.uk/information/what-cyber-incident>.



First and foremost, entities shall assess whether their activity fall under the directive scope of application. As illustrated before, the NIS 2 provides a size-cap rule plus sector specific list in order to categorize entities under essential or important group. The proper classification is not only necessary to understand the cyber-risk management regime applicable (which for both essential and important entities is essentially the same), but also to learn the competent supervisory regime applicable to the case. In fact, the NIS 2 makes a distinction between a full-rounded supervisory regime⁴³ (i.e., ex-ante and ex-post control) for essential entities and lighter supervisory regime⁴⁴ (only ex-post) for important entities. This means that falling under the latter scenario, the entity wouldn't need to routinely document compliance with cybersecurity risk management requirements, and, as a result, the supervisory won't have general obligation to supervise those entities during their activities.

Second, even entities falling outside the Directive scope shall address whether their clients or supplier are still subject to it. This because, their clients or supplier have the obligation to take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedure.⁴⁵ Hence, it won't be enough to fall outside the scope of the NIS 2 to disregard cybersecurity requirements, because it could be imposed on entities from their clients or suppliers. For the same token, all entities subject to the NIS 2 shall evaluate what requirements must they include in their contracts with suppliers or consumers in order to provide a smooth supply chain that complies with the new cybersecurity rules.

Third, companies subject to the NIS 2 shall duly understand their stance and what new requirements would need to be implemented. As showed, certain entities identified by the Commission might be obliged to purchase ICT services or products with specific certification. This means that it might not be possible for some entities to just reproduce their IT infrastructure abroad because some products and services won't be available for sure over there. For this reason, it is important to duly create an inventory of devices and services currently deployed in Europe and re-assess whether they would be available for use once the NIS 2 became effective and the member states implemented it.

Last but not least, entities shall promptly look at the member states in which they operate to evaluate additional cybersecurity compliance requirements and specific standard. As mentioned before, the NIS 2 as a Directive would need to be implemented by Member States who will have until October 2024 to adopt their national legislation. Consequently, many members are now amending their internal rules and promoting higher cybersecurity standards among their economic operators. In this sense, the above-mentioned "cybersecurity perimeter" from Italy or the German *Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (ITSiG 2.0)*.⁴⁶ All entities shall duly identify the Member State that would have jurisdiction on their operation in Europe and duly learn the specific implementation rules related to NIS 2.

Failing to comply with the new rules might result in important penalty to the entities and, in some cases, against the responsible person. The Directive establishes a system of maximum fine and mandates that Members States apply administrative fines as well. In case of violations of the cybersecurity risk management or reporting duties, the normative provides a distinction between essential entities and important entities businesses. For example, an administrative penalty of at least 10,000,000 EUR or 2% of the entire worldwide annual revenue, whichever is larger, should be imposed on violations by the Directive by essential entities.⁴⁷ However, a lower administrative fine of at least 7,000,000 EUR or 1.4% of the worldwide annual revenue should be imposed on important

⁴³ Article 32 of the NIS 2.

⁴⁴ Article 33 of the NIS 2.

⁴⁵ Article 21 Paragraph 3 of NIS 2.

⁴⁶ Schmitz-Berndt and Chiara, "One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive"

⁴⁷ Article 34 Paragraph 4.

entities for violation of the discipline.⁴⁸ In addition, under certain conditions, the national competent authorities with responsibility for supervision and enforcement may ask the appropriate bodies or courts to temporarily prohibit anyone holding the position of chief executive officer or legal representative in that essential entity from performing managerial duties within that entity⁴⁹

5. Conclusion


In conclusion, the coming into force of NIS 2 is set to have a significant impact on all businesses in Europe due to its over-reaching scope of application, which would target even entities beyond the perimeter of the previous discipline of NIS 1 enacted just few years ago. At the same time, all entities falling under the new rules would have to adjust their operation to the new risk management requirements and supervision by competent authorities. The NIS 2 discipline in this regard goes beyond what was achieved before and provides a list of minimum technical, operational and organizational measures to be implemented for controlling cyber risks as well as an obligation to guarantee a degree of security of network and information systems proportionate to the risk presented, taking into account the “state of the art”. Nevertheless, all business could take advantage of what they have learned with the NIS 1 and improve their current security maturity level and practice where required.

Bibliography

- [1] Reuters Media. “China’s Mindray to Buy Diagnostic Test Material Supplier HyTest for \$661 Mln.” May 17, 2021. Accessed November 27, 2022. <https://www.reuters.com/business/healthcare-pharmaceuticals/chinas-mindray-buy-diagnostic-test-material-supplier-hytest-661-mln-2021-05-17/>.
- [2] “Commission Staff Working Document Impact Assessment Report Accompanying the Document 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.” SWD/2020/345 final, European Commission, December 16, 2020. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0345>.
- [3] Council of the European Union. “EU Decides to Strengthen Cybersecurity and Resilience Across the Union: Council Adopts New Legislation.” News release. December 1, 2022. Accessed December 1, 2022. https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/?utm_source=dsms-auto&utm_medium=email&utm_campaign=EU+decides+to+strengthen+cybersecurity+and+resilience+across+the+Union%3a+Council+adopts+new+legislation.
- [4] Daily, Investor’s B. “Nio, BYD, China EV Makers Make Historic Push into Europe.” Investor’s Business Daily, September 30, 2022. Accessed November 27, 2022.
- [5] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measure 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). 65. December 27, 2022. Accessed January 1, 2023. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555&from=IT>.
- [6] European Commission. 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., 2020, COM/2020/823 final. Accessed November 26, 2022. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN>.
- [7] European Parliament. “Cybersecurity: Parliament Adopts New Law to Strengthen EU-Wide Resilience.” News release. December 1, 2022. Accessed December 1, 2022. <https://www.europarl.europa.eu/news/en/press-room/20221107IPR49608/cybersecurity-parliament-adopts-new-law-to-strengthen-eu-wide-resilience>.
- [8] “General Data Protection Regulation (GDPR) Compliance Guidelines.” Accessed November 27, 2022. <https://gdpr.eu/>.
- [9] Gruber, Andreas, and Natalie Ségur-Cabanac. “Necessary or Premature? The NIS 2 Directive from the Perspective of the Telecommunications Sector.” *International Cybersecurity Law Review* 2, no. 2

⁴⁸ Article 34 Paragraph 5.

⁴⁹ Article 32 Paragraph 5 point (b) of NIS 2.

- 
- (2021): 233-43. doi:10.1365/s43439-021-00035-6. <https://link.springer.com/article/10.1365/s43439-021-00035-6>.
- [10] “Joint Communication to the European Parliament and the Council—The EU’s Cybersecurity Strategy for the Digital Decade.” JOIN (2020) 18 final, European Commission, December 16, 2020.
 - [11] Kratz, Agatha, Max Zenglein, Gregor Sebastian, and Mark Witzke. “Chinese FDI in Europe: 2021 Update.” MERICS; Rhodium Group, April 27, 2022.
 - [12] Schmitz-Berndt, S. “European Union · Cybersecurity Is Gaining Momentum - NIS 2.0 Is on Its Way.” *European Data Protection Law Review* 7, no. 4 (2021): 580-85. doi:10.21552/edpl/2021/4/14. <https://edpl.lexxion.eu/article/EDPL/2021/4/14>.
 - [13] Schmitz-Berndt, Sandra, and Pier G. Chiara. “One Step Ahead: Mapping the Italian and German Cybersecurity Laws Against the Proposal for a NIS2 Directive.” *International Cybersecurity Law Review* 3, no. 2 (2022): 289-311. doi:10.1365/s43439-022-00058-7.
 - [14] Shaping Europe’s digital future. “The Digital Services Act Package.” Accessed November 27, 2022. <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>.
 - [15] Sievers, Thomas. “Proposal for a NIS Directive 2.0: Companies Covered by the Extended Scope of Application and Their Obligations.” *International Cybersecurity Law Review* 2, no. 2 (2021): 223-31. doi:10.1365/s43439-021-00033-8. <https://link.springer.com/article/10.1365/s43439-021-00033-8>.
 - [16] Tartar, Andre, Mira Rojanasakul, and Jeremy S. Diamond. “How China Is Buying Its Way into Europe.” Accessed February 4, 2022. <https://www.bloomberg.com/graphics/2018-china-business-in-europe/>.
 - [17] Turak, Natasha. “China Is Investing 9 Times More into Europe Than into North America, Report Reveals.” CNBC, July 17, 2018. Accessed February 4, 2022. <https://www.cnbc.com/2018/07/17/china-is-investing-9-times-more-into-europe-than-into-north-america.html>.
 - [18] National Cyber Security Centre. “What Is a Cyber Incident.” Invalid DateTime. Accessed November 29, 2022. <https://www.ncsc.gov.uk/information/what-cyber-incident>.