The new NIS II Directive and its impact on small and medium enterprises (SMEs): initial considerations*

Elena Kaiser

Abstract

This article examines the impact of the new obligations set forth in directive (EU) 2022/2555 (NIS II) on small and medium enterprises (SMEs). SMEs represent 99% of all businesses in Europe and are crucial to the Digital Single Market. However, despite their importance, these companies still lack the necessary cybersecurity measures to resist and respond to major cyberattacks.

Summary

Keywords

NIS directive – security of network and information systems – small and medium enterprises (SMEs) – impact

1. Introduction

Small and medium enterprises (SMEs), which represent 99% of all businesses in the European Union, are the backbone of the Digital Single Market.[1]
According to the definition given by Eurostat, small enterprises are defined as entities

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

[1] Eurostat, *EU small and medium-sized enterprises: an overview*, in *ec.europa.eu*. In 2018 there were approximately 25 million SMEs in the European Union. See ENISA, *Cybersecurity for SMEs - Challenges and Recommendations*, 2021, in *enisa.europa.eu*, 2021, 9.

having fewer than 50 employees and an annual turnover of less than or equal to €10 million. In contrast, medium-sized companies are defined as having a maximum of 250 employees and a yearly turnover of less than or equal to €50 million.[2] Finally, entities with less than 10 employees and an annual turnover of less than or equal to €2 million are considered micro-enterprises.

Despite their importance in the economic market, most SMEs still need to improve their cybersecurity capacities. According to surveys conducted by the European Commission analyzing the impact of the EU directive concerning the security of network and information systems (NIS I Directive) on entities within the EU, only 27% of small enterprises had an ICT cybersecurity policy in place, compared to 51% of medium enterprises and 72% of large enterprises[3].

SMEs are often targeted by cybercriminals due to low cybersecurity awareness and inadequate incident response programs, which make them easy targets for attacks. Contrary to the common belief that cyber-attacks only occur in large organizations, SMEs may be crucial components of broader supply chains or provide services to critical entities[4]. Additionally, most SMEs process critical information, defined as «information that if it is stolen or lost, the organization would face serious legal repercussion, and the owners of the personal information could encounter significant or even irreversible consequences (...)».[5]

This article provides some initial considerations on how the new European directive concerning the security of network and information systems (NIS II Directive)[6] will affect SMEs. The NIS II was adopted by the European Council on December 14, 2022 and came into force on January 16, 2023. The new legal framework broadens its scope and introduces new compliance obligations and notification requirements, which will be discussed in the following paragraphs.

It is essential to highlight that the NIS II Directive still needs to be implemented at the national level by Member States, as required by European law. Due to the current early stages of the directive's implementation, it can be challenging to obtain a complete and precise overview of the costs and impact on the entities falling under its scope.

The impact assessment will be supported by the documents drafted by the European Commission accompanying the negotiation of the new directive, and by evidence gathered from reports and other initiatives supported by the European Union Agency for Cybersecurity (ENISA).

---

[2] European Commission, *SME*, in *single-market-economy, ec.europa.eu/smes/sme-definition_en.*

[3] G. Endrodi - G. Maridis - S. Schmitz, et. al., *Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)*, 2021, 97, in *data.europa.eu.*

[4] ENISA, *Cybersecurity for SMEs - Challenges and Recommendations,* 2021, 8, in *enisa.europa.eu.*

[5] Ivi, 12.

[6] 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).

2. From NIS I to NIS II

On July 6, 2016, the European Parliament approved the NIS Directive (EU) 2016/1148[7], which is the first horizontal legal instrument aimed at improving cybersecurity resilience in the European internal market. The directive imposes new obligations on Member States to adopt a national cybersecurity strategy, designate one or more national cybersecurity incident response teams (CSIRTs), establish a competent national authority to implement and supervise the directive and appoint a single point of contact for transnational cooperation. Additionally, to promote swift and effective operational cooperation among Member States, including information sharing, the directive establishes a network of national CSIRTs. Finally, it introduces new security and notification requirements.

Regarding its scope, the NIS I Directive distinguishes between "operators of essential services" and "digital service providers". Operators of essential services (OES) are those that belong to sectors and subsectors listed in Annex II, such as energy, transport, banking, financial market infrastructures, health sector, water, and digital infrastructures, and that meet the following criteria: a) providing a service that is essential for the maintenance of critical societal and economic activities; b) the provision of that service depends on network and information systems; c) an incident would have significant disruptive effects on the provision of that service.[8] On the contrary, digital service providers (DSPs) are legal entities that provide digital services listed in Annex III, such as online marketplaces, online search engines, and cloud computing services. Member States bear the responsibility of identifying OESs operating within their territories.[9] However, the NIS Directive fails to provide any precise mechanism to identify such OESs or establish standard criteria based on their size.[10] Additionally, Member States are not obligated to identify DSPs. As a result, some entities that play an essential role in the digital market and which certain OESs rely on to provide their services, such as cloud service providers, are beyond the scope of competent national authorities' supervision.

The lack of an identification procedure for OESs and DSPs reflects the minimum harmonization criterion, which the directive adopts as a general approach for all its obligations and mechanisms.

The NIS I sets only generic objectives, giving Member States the freedom to choose measures to adopt at the national level to achieve these goals. However, this broad discretion led to inconsistent and inefficient implementation of the directive among Member States.

Besides the aforementioned issues with identifying OESs and DSPs, other critical

[7] 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.

[8] Art. 5, directive (EU) 2016/1148.

[9] According to art. 5, para. 1, directive (EU) 2016/1148, by 9 November 2018, Member States shall identify the operators of essential services with an establishment on their territory for each sector and subsector referred to in Annex II.

[10] See also T. Sievers, *Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligation*, in *International Cybersecurity Law Review*, 2021, 225-226.

issues have emerged concerning the incident notification and sanction system. For instance, the lack of specific parameters for measuring "the significance or substance of an incident" that triggers the notification obligations to competent authorities or CSIRTs, has contributed to underreporting of incidents and a lack of coordinated crisis response.[11]

Additionally, non-specified security obligations have resulted in inconsistent levels of cybersecurity awareness and resilience across Member States and sectors. Finally, the penalty system has been undetermined[12]: penalties for non-compliance with the provisions of the NIS Directive have differed significantly among Member States and, in some cases, were almost non-existent.[13]

Furthermore, the digital transformation of society, intensified by the COVID-19 crisis, has expanded the threat landscape with increased and more sophisticated attacks originating from both within and outside the European Union. The cybersecurity directive has been incapable of addressing these new challenges.[14]

The necessity to harmonize the NIS Directive and its insufficiency in dealing with emerging cyber threats made it imperative to adopt a new legal text to enhance and ensure cybersecurity resilience within the European Union. The Council of the European Union approved the final text of the NIS II Directive in December 2022, and it came into force on 16 January 2023. This new regulatory framework, along with the Critical Entities Resilience (CER) Directive[15], is a crucial policy pillar of the so-called "European Cybersecurity Strategy for the Digital Decade".[16]

2.1 NIS II and the size-cap rule

While NIS I differentiated between operators of essential services and digital service providers, the recently approved NIS II replaces these categories with essential and important services and significantly expands the list of entities and sectors falling under its scope.

The method of supervision, kept from the previous directive, is the main distinguishing factor between essential and important entities: for the first category, the control

[11] G. Endrodi - G. Maridis - S. Schmitz, et. al., *Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive*), cit., 46.

[12] Art. 21, directive (EU) 2016/1148, only indicates that penalties shall be effective, proportionate, and dissuasive.

[13] G. Endrodi - G. Maridis - S. Schmitz, et. al., *Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive*), cit., 54 ss.

[14] 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.

[15] 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.

[16] European Commission, *The EU's Cybersecurity Strategy for the Digital Decade*, 16 December 2020, in *digital-strategy.ec.europa.eu*.

is more rigorous and covers both *ex ante* and *ex post* aspects. In contrast, for important entities, supervisory powers intervene only when there is evidence that the organization did not comply with its risk management and notification obligations (*ex post*).[17]
Unlike the NIS I Directive, which allowed Member States to determine the entities recognized as OES, the new NIS II Directive introduces a unique criterion based on the size of the entity, known as the "size-cap" rule. According to this rule, all medium and large entities operating in sectors or providing services listed in Annex I and II of the directive fall within its scope by default.
Furthermore, companies must determine for themselves whether they are essential or important entities, "as a determination made by the national competent authority (NCA) is no longer required".[18]
As for the size threshold, the directive is clear: it applies to entities that meet or exceed the thresholds for medium-sized enterprises.[19] Consequently, micro and small enterprises are, generally, excluded from its scope.
However, there are broad exceptions to this criterion. According to art. 2, the directive always applies, regardless of the size, to providers of public electronic communications networks or publicly available electronic communications services[20], trust service providers, top-level domain name registries, or system service providers.
In addition, national authorities can identify also micro and small entities as essential or important if they are the only service provider, have a significant impact on public safety and security, perform a vital function for society, or are important at the national or regional level. Public administrations can also be identified as essential or important, regardless of their size, if they are central governments or provide significant services.
Finally, the exemption also applies to entities identified as critical according to the CER Directive and to entities providing domain name registration services.
Based on these elements of analysis, the list of entities that may be considered essential or important is much broader than in the past, and it may even include entities such as public administrations that were entirely excluded from the scope of the previous directive.
While NIS I did not explicitly mention size criteria for its applicability, certain SMEs, particularly those of medium size, were already deemed operators of essential services by the competent national authorities of Member States, primarily in smaller European countries. However, the establishment of medium size as the general criterion

[17] Artt. 32 and 33, directive (EU) 2022/2555.

[18] T. Sievers, *Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligation*, cit., 226.

[19] Art. 2, para. 1, directive (EU) 2022/2555.

[20] Providers of public electronic communications networks or publicly available communications services are already subject to regulation under the European Electronic Communication Code (directive (EU) 2018/1972) which includes high-security standards. Similarly, trust service providers would be exempt from the size cap rule as some security standards are already implemented within the eIDAS framework (regulation (EU) 910/2014). Excluding micro and small providers from the NIS scope may have a negative impact on these existing standards.

under NIS II may substantially expand the number of entities subject to new cybersecurity compliance obligations, potentially resulting in increased costs and burdens that may prove challenging to manage.

2.2 The new role of SMEs in the directive

As mentioned earlier, the size of an entity was not a criterion for applying or excluding NIS I. Therefore, even though some SMEs were playing critical roles as digital service providers in certain Member States, the previous directive did not make any explicit reference to them. The only exception is contained in Recital 40, which states that «Information about incidents is increasingly valuable to the general public and businesses, particularly small and medium-sized enterprises».
On the contrary, NIS II recognizes that strengthening the cyber resilience and cyber hygiene baseline of SMEs, especially those excluded from the directive's scope, is a key policy element that must be addressed in the national cybersecurity strategies of Member States. In particular, resilience shall be strengthened by providing «easily accessible guidance and assistance for their specific needs».[21] In order to assist small and medium-sized enterprises in tackling their cybersecurity challenges, Member States should implement a range of measures, including the establishment of a national point of contact and the provision of operational services such as website configuration and logging.[22]
As per the new directive, the European Union Agency for Cybersecurity (ENISA) is responsible for evaluating the cybersecurity awareness level among small and medium-sized enterprises at the European level. The findings of this research will be included in the biennial report on the status of cybersecurity in the Union, which is prepared in collaboration with the European Commission and the Cooperation Group and presented to the European Parliament.[23]

3. What are the new obligations for SMEs falling under the directive's scope?

Alongside the new categorization of essential and important entities and a broader area of application, the NIS II established new obligations and cooperation mechanisms.
The new principles and obligations established by NIS II are numerous and complex. Therefore, it is crucial to ensure that Member States, as well as essential and important entities falling under the new legal framework, have the necessary resources to comply with them.
NIS II introduces a new crisis management framework (art. 9), new tasks and require-

[21] Art. 7, part. 2, lett. i), directive (EU) 2022/2555.

[22] Recital 56, directive (EU) 2022/2555. See also ENISA, *Cybersecurity for SMEs, Challenges and Recommendations*, cit., 14 ss.

[23] Art. 18, para. 1, lett. c), directive (EU) 2022/2555.

ments for national CSIRTs (art. 11), a coordinated vulnerability disclosure mechanism (art. 12), and the European Cyber Crisis Liaison Organization Network (EU-CyCLONe) for the management of large-scale European cybersecurity incidents (art.16). However, these new obligations mainly impact national authorities, CSIRTs, and all entities in charge of crisis management.

On the other hand, essential and important entities, which may also include SMEs, are obligated to comply with risk management measures and reporting obligations.

While art. 14 of NIS I generally referred to «security requirements and incident notifications», the new text dedicates the entire Chapter IV to «Risk management measures and reporting obligations», which includes five articles: governance, cybersecurity risk management measures, coordinated security risk assessment of supply chains, reporting obligations, and the use of European cybersecurity certification schemes.

According to NIS I, operators of essential services and digital service providers should take appropriate and proportionate technical and organizational measures to manage risks posed to the security of network and information systems and adopt proper measures to mitigate the impact of incidents affecting the security of such systems.[24] In addition, OESs and DSPs were required to promptly notify the competent authority or the national CSIRT if they experience incidents that had a significant impact on the continuity of essential services or that substantially affect the provision of their online marketplace, online search engine, or cloud computing service within the Union. The criteria used to assess whether an incident was of significant or substantial impact could include the number of affected users, the incident's duration, and the geographical extent.[25]

However, as highlighted above, such obligations were too undetermined. As a consequence, security requirements differed significantly across Member States. Additionally, the lack of understanding regarding the time and notification process, as well as the threshold triggering it, led to many unreported incidents.[26]

[24] Art. 14, paras. 1 and 2; art. 16, paras. 1 and 2, directive (EU) 2016/1148.

[25] Art. 14, paras. 3 and 4; art. 16, paras. 3 and 4, directive (EU) 2016/1148.

[26] Although the Cooperation Group provided guidelines on the security requirements and notification mechanisms for both OESs and DSPs, Member States adopted different approaches, resulting in varying levels of security and a lack of harmonization in incident response. Reference document on security measures for Operators of Essential Services, available at *digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group*. G. Endrodi - G. Maridis - S. Schmitz, et. al., *Study to support the review of Directive (EU) 2016/1148 concerning measures foir a high common level of security of network and information systems across the Union (NIS Directive)*, cit., 15. Additional elements to determine security requirements and the substantial effect of a cybersecurity incident for digital service providers are provided by the European Commission Implementing Regulation 2018/151 of 30 January 2018 laying down rules for application of directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact. See also D. Markopoulou - V. Papakonstantinou - P. de Hert, *The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation*, in *Computer Law & Security Review*, 2019, 4.

3.1. Cybersecurity risk management measures

In line with the previous directive, art. 21, para. 1, NIS II establishes that security measures should be adopted to manage and mitigate risks posed to the security of network and information systems and to prevent and minimize the impact of incidents. «The main objective of these measures should be to ensure the continuity of such services».[27]

The novelty lies in para. 2 of art. 21, which outlines a detailed list of minimum measures that entities must adopt. This list of criteria can contribute to a more harmonized approach among Member States, which was missing in the previous directive, and promote generalized cyber resilience among all entities operating in the European Union. The required cybersecurity measures include a) conducting risk analysis and developing information system policies establishing; b) incident handling procedures; c) implementing backup and crisis management plans, ensuring disaster recovery to maintain business continuity; d) securing the supply chain; e) ensuring network and information system security during acquisition, development, and maintenance, including vulnerability handling; f) establishing policies and procedures to assess the effectiveness of cybersecurity risk-management measures; g) promoting basic cyber hygiene practices; (h) implementing policies and procedures for the use of cryptography and encryption; (i) human resources security and (j) multi-factor authentication. Failure to comply with these measures may result in the adoption of necessary, appropriate, and proportionate corrective measures by Member States.[28]

The utilization of ICT products, services, and processes that hold cybersecurity certification under the provisions of regulation (EU) 2019/881 (also known as the Cybersecurity Act) is a means to exhibit conformity with the aforementioned obligations.[29]

3.2 Reporting obligations

Art. 23 of the new directive sets out comprehensive reporting obligations for essential and important entities, which entail specific timelines, content requirements, and the involvement of CSIRTs in the reporting process. This reporting mechanism bears similarities to the one described in art. 33 of the General Data Protection Regulation (GDPR).[30]

States must promptly notify CSIRTs or the competent authorities of incidents that significantly affect the provision of their services. An incident qualifies as having a significant impact if it has resulted in or could result in severe operational disruption

[27] D. Markopoulou - V. Papakonstantinou - P. de Hert, *The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation*, cit., 3.

[28] Art. 21, para. 4, directive (EU) 2022/2555.

[29] Art. 24, paras. 1 and 2., directive (EU) 2022/2555.

[30] 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.

of the services or financial loss for the concerned entity, or if it has caused or could cause considerable material or non-material damage to other natural or legal persons.
An entity affected by a cybersecurity incident that causes a significant impact must provide the CSIRT or competent authority with the following:
a) An early warning, indicating whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact. This warning must be provided without undue delay and, in any event, within 24 hours.
b) An incident notification within 72 hours of becoming aware of the significant incident. The notification should include an initial assessment of the incident's severity and impact.
c) An intermediate report upon request of the CSIRT.
d) A final report not later than one month after the incident notification submission. The final report should include a detailed description of the incident, the type of threat or root cause likely to have triggered the incident, mitigation measures that have been applied, where applicable, and the cross-border impact of the incident.
Upon receiving the early warning, the CSIRT or competent authority shall provide, where possible, a response to the notifying entity within 24 hours, including initial feedback and, upon request, operational advice on possible mitigation measures.
Moreover, both essential and important entities, as well as entities that are not covered by this directive, can always voluntarily report any significant incidents, cyber threats, or near misses.[31]

3.3 Penalties and enforcement measures

Art. 34 of the NIS II introduces a sanction scheme that provides maximum penalties for non-compliance with the directive obligations, similar to what is already done in the GDPR. In contrast, the previous directive delegated Member States to adopt rules on infringements of national laws transposing the directive and imposed a general obligation for these measures to be effective, persuasive, and dissuasive. As noted above, penalties for non-compliance with the NIS Directive varied greatly among Member States in both characteristics and severity.
The NIS II Directive sets the threshold for administrative fines that Member States must impose on essential and important entities that fail to comply with cybersecurity measures and reporting obligations.
Non-compliance with art. 21, which concerns cybersecurity risk-management measures, and art. 23, which concerns reporting obligations, results in:
For essential entities: an administrative fine of a maximum of at least EUR 10 000 000 or a maximum of at least 2% of the total worldwide annual turnover.
For important entities: an administrative fine of a maximum of at least EUR 7.000.000 or a maximum of at least 1,4% of the total worldwide annual turnover[32].
If we compare these figures with the average financial capacity of small and medium

[31] Art. 30, para. 1, lett. a) - b), directive (EU) 2022/2555.

[32] Art. 34, paras. 4 and 5, directive (EU) 2022/2555.

size businesses, it becomes evident that these new penalties are significantly high and can have a considerable impact on their business continuity.
Besides administrative fines, essential and important entities are also subjected to supervisory and enforcement measures by competent national authorities, which can also lead to adopting corrective measures and administrative fines.
As mentioned above, for essential entities, the supervision is both *ex ante* and *ex post*, while for the important entities, it is only *ex post*. This different method of supervision is kept from the previous directive. Supervisory tasks include on-site inspections, regular and target security audits, or requests to access data[33].
If the supervisory activities described above ascertain any violation of the obligations laid down by the directive, competent authorities also exercise enforcement powers to ensure compliance with such obligations. According to arts. 32 and 33, these measures include warnings about infringements; orders of ceasing conducts infringing the directive; orders of compliance with cybersecurity risk-management measures and reporting obligations; orders of providing information to the natural or legal persons potentially affected by a cyber threat; orders of designating a monitoring officer to oversee the compliance of cybersecurity risk-management measures and of reporting obligations. Finally, competent national authorities may impose or request relevant bodies or tribunals to impose administrative fines under art. 34 NIS II Directive.

4. Impact and costs of the new directive on SMEs: initial considerations

Due to the broader scope of the new directive, which includes sectors and entities that were previously excluded from the application of NIS II, and the numerous exceptions to the size-cap rule, more companies, including micro and small, will have to comply with European obligations. At the same time, according to the general rule established by art. 2, it is expected that new medium-sized enterprises will have to comply with the obligations established by NIS II.
As a general rule, small and micro enterprises are explicitly excluded from the scope of the directive. However, Member States may choose to extend the directive's scope to include those that are deemed critical to the functioning of essential services. In such cases, the costs and impact of NIS on small and micro enterprises will need to be carefully evaluated to ensure that the benefits outweigh the costs.
While micro-enterprises rarely provide public electronic communication networks, trust services providers, or other essential and important services to a country, except for some small Member States, small and medium enterprises may provide essential services and even become suppliers of critical entities.
It is widely known that in the technological sector, the size of an organization does not necessarily reflect its importance in a particular economy or the quantity and relevance of the data it processes.
Additionally, SMEs can play a crucial role in supply chains. In this regard, essential

[33] Artt. 32 and 33, directive (EU) 2022/2555.

concerns have been raised during the negotiation process of the NIS II Directive. In particular, the European DIGITAL SME Alliance has stated that:
«While the NIS2 directive excludes small and micro enterprises from having to comply with the directive, the need for supply chain security and the requirement for entities to ensure that their supply chains and service providers are cybersecurity could lead to small and micro enterprises having to prove compliance with the directive, in order to retain business relationships. The forthcoming risk assessment should ensure that security requirements for service providers and manufacturers in the supply remain proportionate and realistic, relative to the level of threat and vulnerability (...)».[34]
It is, therefore, of utmost importance to support not only micro and small entities that will fall within the scope of the directive but also those that will be excluded from it and, as a result, are precluded from awareness campaigns, projects, and funding.
The NIS II tasks the European Commission, in cooperation with the Cooperation Group, to provide guidelines to SMEs to assess whether they fall within the directive's scope and to support them in this regard.[35] However, as the NIS II text has only recently entered into force and still needs to be implemented by Member States through national legislation, it is presumed that these guidelines will be provided in the coming months.
Various assessment reports conducted by the European Commission, which accompanied the proposal for the new directive[36], highlighted an insufficient application of cyber resilience and risk management practices by SMEs. Small companies often lacked financial and human resources, staff, and awareness to provide adequate cybersecurity. The concern with a small company arose mainly when they had access to or relate to more significant targets, thus becoming vectors for cyber-attacks on more critical targets.[37]
According to another survey carried out by ENISA, many SMEs already had some cybersecurity measures in place even before the COVID-19 crisis, which heavily impacted their business continuity and exposed them to new risks mainly due to remote working. However, such measures were mostly basic technical controls, such as antivirus software.[38] Notwithstanding the low level of cybersecurity capacity, SMEs within the European Union understood that cybersecurity was an important issue and that

[34] European DIGITAL SME Alliance, *Digital SME input to the consultation of the proposal for a revised directive on the Security of Network and Information systems (NIS 2 Directive)*, in *digitalsme.eu,* 2021.

[35] Recital 20, directive (EU) 2022/2555.

[36] Parts 1, 2, 3 of the 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.

[37] Supply chain attacks are increasing in terms of frequency and strength. For much information concerning the threat landscape, ENISA *Threat landscape for supply chain attacks*, in *enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks*, 2021. The level of resilience and risk management practices applied by SMEs varies across different sectors. For example, the health sector, which has been significantly affected by the COVID-19 crisis, is now covered by more specific elements under NIS II (Annex I), including entities involved in research and development of medicinal products and those manufacturing medical devices. Annex I, directive (EU) 2022/2555.

[38] ENISA, *Cybersecurity for SMEs, Challenges and Recommendations*, cit., 28.

they relied on their ICT infrastructure.[39]

The European legislator shall generally require Member States to establish frameworks for raising awareness of cyber threats among SMEs and supporting them in confronting those threats. This need is reflected in art. 7 of the new NIS II Directive, which mandates national cybersecurity strategies to adopt specific policies that strengthen cyber awareness and hygiene among SMEs. However, the question remains whether this provision alone will sufficiently address all the challenges faced by SMEs in terms of cyber resilience and costs.

At this early stage, it is ambitious to assess the concrete impact and costs of NIS II on such enterprises, given that the new text entered into force only in January. Data on the number of medium and small-sized enterprises that fall under the scope of NIS as essential or important entities are, in fact, not yet available. It is also unclear how many of these companies were previously considered OESs or DSPs under NIS I and had, therefore, sufficient cybersecurity measures already in place.

It is estimated companies falling under the scope of the directive, which certainly include medium-sized enterprises, will need to increase their current ICT security spending by a maximum of 22% over the next few years[40], with compliance costs being the most significant. These costs are primarily related to fulfilling the risk management obligations outlined in art. 21, complying with reporting obligations under art. 23, and documenting compliance with supervisory and enforcement measures imposed by competent authorities.[41]

At the same time, raising the level of security requirements for these entities would also incentivize their cybersecurity capabilities and help improve their ICT risk management. However, currently, there are no comparable data available across the EU to measure the return on security investment (ROSI) at the company level, either across sectors or per sector.[42]

5. ENISA's role and SMEs

In June 2019, the European Cybersecurity Act came into force, which established a European cybersecurity certification scheme and granted a permanent mandate to the European Union Agency for Cybersecurity (ENISA).[43]

ENISA's mandate encompasses providing support to Member States and Union institutions to enhance cybersecurity and reduce internal market fragmentation[44], which

[39] Ivi, 3. According to the survey, over 80% of the SMEs stated that cybersecurity issues would seriously impact their business within a week of the problems happening, with 57% saying that they would most likely go bankrupt or go out of business.

[40] 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, cit., part. ⅓., 72.

[41] Ivi, 74.

[42] Ivi, 69.

[43] Established in 2004.

[44] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on

includes assisting with the transposition of NIS I into national legislation.

The NIS II Directive has expanded ENISA's role in the network and information security context, and it is now responsible for the following:

- Developing and maintaining a European vulnerability database[45];
- Assisting in developing CSIRTs, if requested by Member States[46];
- Provide the secretariat to the CSIRTs network[47] and the EU-CyCLONe[48];
- Carrying out a coordinated security risk assessment of supply chains in cooperation with the Cooperation Group and the Commission[49];
- Developing guidance on security requirements and reporting obligations for providers of public electronic communications networks or publicly available electronic communications services to facilitate harmonization and transition[50];
- Creating and maintaining a registry 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 and of social networking services platforms[51];
- Supporting the establishment of cybersecurity information-sharing arrangements exchanging best practices and providing guidance[52].

Moreover, as part of its duties under NIS II, the European Cybersecurity Agency is responsible for producing a biennial report on the state of cybersecurity in the European Union, which includes an evaluation of the level of cybersecurity awareness and hygiene among small and medium enterprises.

Since 2006, even before the permanent mandate given by the Cybersecurity Act, the European Agency has been promoting initiatives to support SMEs and Member States in elevating their level of understanding of cybersecurity risks and threats (such as phishing and ransomware), raising awareness, and promoting best cybersecurity practices.[53]

More recently, in 2021, ENISA published a report called "Cybersecurity for SMEs -

ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

45 Art. 12, para. 2, directive (EU) 2022/2555; recital 60, directive (EU) 2022/2555.

46 Art. 10, para. 10, directive (EU) 2022/2555.

47 Art. 15, para. 2, directive (EU) 2022/2555.

48 Art. 16, para. 2, directive (EU) 2022/2555.

49 Art. 22, directive (EU) 2022/2555 ; recital 90, directive (EU) 2022/2555.

50 Recital 95, directive (EU) 2022/2555.

51 Art. 27, directive (EU) 2022/2555; recital 117, directive (EU) 2022/2555.

52 Art. 29, para. 5, directive (EU) 2022/2555.

53 Between 2006 and 2015, the Agency published several reports aimed at supporting SMEs in managing cybersecurity risks, including two Information Package for SMEs reports providing risk assessment and management methodologies, a Business Continuity for SMEs report facilitating IT knowledge transfer, and a Cloud Security Guide for SMEs report addressing security risks and opportunities related to cloud services. These reports can be accessed at *enisa.europa.eu.*

Challenges and Recommendations"[54], which advises SMEs on measures to improve their cybersecurity resilience and suggests concrete actions for Member States to support them in this process. The report highlights how the COVID-19 crisis exacerbated existing challenges and provides guidelines for mitigating them. ENISA has identified the main challenges for SMEs as low cybersecurity awareness and management support, inadequate protection for critical and sensitive information, budgetary issues, lack of ICT cybersecurity expertise and personnel, lack of appropriate guidelines.[55] The most frequent incidents experienced by SMEs include ransomware attacks on their service providers or PCs, theft of laptops, and CEO fraud[56]. The report provides recommendations addressing three main areas and levels: people, processes, and technology.

A short practical guide called "Cybersecurity Guide for SMEs" accompanies the report, providing 12 high-level steps to better secure SMEs' systems and their business.[57] In the same year, ENISA also promoted the "SecureSME-cyber tips," which provide short and practical suggestions to protect employees, enhance processes, strengthen technical measures, and overcome all issues companies had to deal with during the COVID-19 pandemic.[58] The portal includes practical videos to aid in this endeavor.

In March 2023, ENISA developed a new "Cybersecurity Maturity Assessment" tool to diagnose SMEs' cybersecurity maturity level.[59] The tool includes essential features, such as a cybersecurity evaluation based on several questions and a personalized action plan that aligns with best cybersecurity practices. Similar to the "Cybersecurity for SMEs" report, the tool focuses on the three key areas: people, technology, and processes.

6. Conclusions

In summary, the NIS II Directive imposes new obligations on a larger number of entities, including SMEs. The directive expands its scope to cover additional sectors and entities and introduces a "size-cap" rule, that sets the minimum threshold for medium and large organizations. As a result, medium-sized enterprises are now included by default in the new legal framework, while micro and small enterprises are generally excluded from its scope.

Art. 2 NIS II Directive lists exceptions where the regulatory framework applies "regardless of the size", such as when entities provide public electronic communications network services, trust services, top-level domain name registries, services with sig-

[54] ENISA, *Cybersecurity for SMEs, Challenges and Recommendations*, 2021, cit.

[55] Ivi, 14 ss.

[56] Ivi, 24 ss.

[57] ENISA, *Cybersecurity guide for SMEs, 12 steps to securing your business*, 2021, in *enisa.europa.eu.*

[58] ENISA, *Secure SME*, 2021, in *enisa.europa.eu.*

[59] ENISA, *Diagnose your SMEs Cybersecurity and Scan for Recommendations*, in *enisa.europa.eu.* See also ENISA, *Cybersecurity Maturity Assessment for Small and Medium Enterprises,* in *enisa.europa.eu.*

nificant impact on public safety and security, or perform vital functions for society. As a result, even micro and small enterprises, which are generally excluded from the directive's scope, may fall under these exceptions. Although micro-enterprises rarely provide essential services, small and medium-sized enterprises can become suppliers of critical entities, making them vulnerable to cyberattacks.

Notwithstanding their importance in the digital market, the general level of cyber awareness and incident management of SMEs is still relatively low. Based on some surveys carried out by the European Commission, only 27% of small enterprises have an ICT cybersecurity policy in place, compared to 51% of medium enterprises.

As for the impact of NIS II on micro and small-sized enterprises, there is no concrete estimation done so far. Additionally, no data is available yet on how many medium and small-sized enterprises that were considered OESs or DSPs according to the previous directive will become essential or important entities. On the contrary, for medium-sized enterprises, it can be expected that there would be an increase in their ICT security spending in the first years following the introduction of the new NIS II framework.

Several initiatives targeting and improving the cybersecurity resilience of SMEs have been promoted at the European level by ENISA. The cybersecurity agency was established in 2004 and received a permanent mandate in 2021 to support Member States and Union institutions in improving cybersecurity and reducing internal market fragmentation, including the implementation of NIS Directive obligations. New functions have been assigned to the Agency by the new directive, including carrying out security assessments of supply chains and developing guidance on security requirements and reporting obligations.

According to NIS II, cybersecurity awareness and hygiene of SMEs have also become vital policy elements that need to be addressed and implemented by Member States through their national cybersecurity strategies.