Employers entrusted to deliver
Sustainability Growth Innovation

Position Paper

Input to the EU rules on the security of network and information systems
Commission proposal (NIS 2 Directive)

18 March 2021

SGI EUROPE GENERAL SECRETARIAT Rue des Deux Eglises, 26 bt 5, BE – 1000 Brussels
T: + 32 (0) 2 219 27 98 | F: + 32 (0) 2 218 12 13 | E: SGIeurope@SGIeurope.org | www.SGIeurope.org
Registered stakeholder
ID Nr 59513031434-92

Employers entrusted to deliver
Sustainability Growth Innovation

Position

Brussels, 18 March 2021

SGI Europe generally welcomes the opportunity to provide feedback to the recently adopted **Directive on security of network and information systems (NIS 2 Directive)** by the European Commission that **introduces in our point of view significant changes** compared with the first version of the Directive.

SGI Europe wishes to take this opportunity to comment on the proposal since it has identified that **the new draft could have a negative impact on many of its members that are providers of services of general interest and subject to the Directive under the provisions of Annex I of the proposed draft.** The main issue lies in the fact **that the entitlement to define the threshold for the application of** the mandatory technical and organisational **measures** that weigh in on these operators **has been withdrawn from Member States (MSs.)** The **Commission now includes all public and private entities in the relevant sectors in the scope of the proposal. The only exception from the scope is for Micro- and Small Enterprise as defined by the** *Commission Recommendation 2003/361/EC*[1]. SGI Europe is **once again forced to point out the unsuitability of the European SME definition, which continues to be a burden for many SGI members all across Europe.**

On a general note, SGI Europe can support the European Commission's global approach to cybersecurity reaffirmed in the "Shaping Europe's Digital Future" communication and welcomes the upcoming revised European Cybersecurity Strategy, including a review of the NIS 2 Directive. We believe that cybersecurity is of paramount importance, especially with the ongoing digitalisation of the entire society and economy that may be accelerated following the current COVID crisis. When designed, cybersecurity policy should take on board existing EU or international standards and good practices by the industry and acknowledge that **there cannot be a one-size-fits-all set of cybersecurity measures.** Cybersecurity challenges and measures vary considerably depending on the sector (e.g. critical infrastructures, government etc.), the type of users (consumers vs. enterprises), the types of data etc.
Several telecommunications operators are active across multiple countries in the European single market. Therefore, SGI Europe calls for a legislative framework that provides for a **high common level of cybersecurity and legal certainty**. A fragmented set of European and national rules would inevitably lead to market distortions and differing security standards.

More specifically, SGI Europe has identified several critical points within the Commission proposal which it would like to address in the following paragraphs:

On **Art. 18, the expanded scope of the proposal would impose a list of mandatory cybersecurity measures on all Local Public Services Enterprises (LPSEs) in the relevant sectors, regardless of size, actual facilities operated or the acute risk of their potential disruption.** Such a lack of differentiation would constitute an excessive burden for a majority of LPSEs, especially the smaller ones.

Thus, SGI Europe strongly recommends giving the MSs the ability to differentiate the cybersecurity measures between sectors, to find **an efficient balance between the desired level of security and the additional burden for the entities affected**. In this context, Art. 18 Paragraph 6 should empower the Commission to adopt implementing acts and not delegated acts. That way, the MS are formally involved in the process and can ensure congruency with existing national cybersecurity rules.

[1] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises

Art. 18 Paragraph 2 Letter d) and Paragraph 3 would make the entities solely responsible for supply chain security. From the perspective of **SGI Europe**, **it is unclear why suppliers and service providers should not share in or solely bear the responsibility for the components and products they provide.** Therefore, the responsibility for supply chain security cannot be imposed solely on entities, especially since smaller LPSEs do not have the resources necessary for scrutiny along the whole supply chain.

Art. 21 Paragraph 2 would empower the Commission to mandate the usage of European cybersecurity certification schemes through delegated acts. **To ensure coherence with national-level standards and schemes and avoid duplication and redundancy, SGI Europe proposes to adhere to the principle of subsidiarity and to only apply European cybersecurity certification schemes in cases where national-level schemes do not exist.** Furthermore, mandatory certification should be limited to critical components only.

Apart from these suggestions related to the content of the proposal, SGI Europe is **once again forced to point out the unsuitability of the European SME, which continues to be a burden for many SGI members all across Europe. A new example of the burden of the SME definition on SGI members through its continued application in legislative proposals by the Commission in the current NIS 2-proposal:**

The current wording of Article 2 reads as follows:

> *"This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC"*

The **current definition of SMEs** under European law is based on the *Commission Recommendation 2003/361/EC*, which has subsequently been embedded in EU binding law by being included in the *Commission Regulation (EU) No 651/2014*. Under this legal framework, **SMEs that are mainly or entirely owned by public authorities —also known as the ownership criterion— do not fall under the European definition of an SME**. This non-recognition has **negative consequences** on their right to benefit from administrative simplification measures, leading to distorted conditions of competition for public SMEs in certain service sectors. **Therefore, all Local Public Services Enterprises (LPSEs), regardless of their size, would fall within the scope of the NIS 2 directive and would not benefit from the exception envisioned for enterprises of their size. In fact,** this situation will **affect all LPSEs** by **restricting their ability to fulfil their mission of general interest** as public services and services of general interest providers. Given their strategic role in the European territories, these public SMEs need to be supported, particularly in the context of economic recovery following the Covid-19 related crisis.

In the **latest position paper on "Rethinking the SME Definition", SGI Europe** already pointed out that the non-recognition of LPSEs as SMEs has serious consequences on their access to administrative simplification measures.

From SGI Europe perspective, the proposal for the NIS-2 Directive is detrimental to its members for several main reasons:

- **As it stands, it would expand the scope of cybersecurity obligations to all entities in the relevant sectors, which are not SMEs under the European definition, regardless of their size. As such, the nearly 32 000 LPSEs in Europe would bear the burden of the complex measures put in place by the proposal.**
- **Furthermore, these entities would be faced with a catalogue of mandatory cybersecurity measures, reporting obligations and potential penalties that stand in contrast with the actual size and capacities of the vast majority of LPSEs. As a reminder, around 97% of LPSEs are SMEs based on**

the staff headcount and financial performance criteria - with 45% of them considered microenterprises.

The urgent need to modify the SME definition

In the same way as other European Regulations affect LPSEs efficient functioning –such as the *Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data*, or *the Directive 2012/27/EU of 25 October 2012 on energy efficiency***–** the NIS-2 Directive is merely further proof of what we have been claiming for years.

Whereas the European Commission does not seem to acknowledge yet the importance of the LPSE model, **SGI Europe is convinced that the modification of the SME definition should be carried out urgently**. Since 2003, the perception of public enterprises has considerably evolved, with an increased awareness that "public" is not equivalent to neither "advantaged", nor "favoured". Indeed, public SMEs are not big companies in disguise, and do not benefit from hidden subsidies or additional staff. Faced with this common misconception, SGI Europe wants to stress out that **LPSEs meet the same challenges than private SMEs of the same size.**

SGI Europe demand is for its LPSE members to be able to benefit from the simplification measures adopted for SMEs at European and MSs level, in accordance with the "think small first" principle enshrined in the European SME development culture since the "Small Business Act" of 2008. **Given its costs and complexity, cybersecurity measures should particularly take into account the type and size of operators upon which it creates obligations.** LPSEs have the strong will to comply with the European rules on security of network and information systems, but have limited capacities to implement them under legal constraint.

Regarding the Commission Recommendation 2003/361/EC, SGI Europe demands:

1. **Amend Article 3(4) of the Annex to Commission Recommendation 2003/361/EC as the benchmark SME definition**, to provide only for the number of employees and the annual turnover or total annual balance sheet criteria. Therefore, the public participation threshold should be removed, and public control should not affect the SME status of a company;
2. **Amend all EU legal instruments, both binding and non-binding**, that refer, directly or indirectly, to this definition, by adjusting them accordingly.
3. **Exclude, under the framework of the NIS 2-Directive, the application of Article 3(4) of the Annex** to Commission Recommendation 2003/361/EC within the proposal for the NIS 2-Directive.

ANNEX

Relevant background of the NIS Directive for SGI Europe

The European Parliament adopted *Directive 2016/1148 on security of network and information systems*[2] (**NIS Directive**) on 6 July 2016. This very important piece of legislation came to **address the complex issue of cybersecurity at European level for the first time.**

The Directive provided a common framework for all MSs to tackle this matter in a coordinated matter. In particular, it **implemented technical and organisational measures** applying to **operators of essential services and digital service providers.** Such measures included in particular:

- The establishment of security and notification requirements for operators of essential services and for digital service providers;
- The guarantee of an appropriate level of security of network and information systems appropriate to the risk posed by those operators; or
- The prevention and minimisation of the impact of incidents affecting the security of their network and information systems.

Under this Directive**, MSs were left with the discretion to define the thresholds above which the operators were concerned by these measures.** This allowed the national transposing legislations to take into account the specific circumstances surrounding the provision of essential and digital services in their territories.

To enforce the execution of these measures by the operators, the Directive provided for "effective, proportionate and dissuasive" penalties to be applied by MSs to any infringement of national provisions adopted pursuant to the Directive [see *Article 21*].

[2] 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