# DIGITAL SME INPUT TO THE CONSULTATION ON THE PROPOSAL FOR A REVISED DIRECTIVE ON SECURITY OF NETWORK AND INFORMATION SYSTEMS (NIS 2 DIRECTIVE)

*15 March 2021*

**Introduction**

With the adoption of the European Commission proposal for a revised Directive on the Security of Network and Information Systems (NIS2 D) on 16 December 2020, the European Commission aims to extend some aspects of the NIS Directive and to harmonise its application further throughout the EU, by providing clarifications, definitions and further explanation to the original version of the Directive.

**DIGITAL SME generally welcomes the clarifications and revisions that have been made to the Directive.** As noted in our previous response to the open consultation, DIGITAL SME was in favour of the efforts to strengthen the harmonisation of the Digital Single Market but remained wary of the negative impact that varying implementations between Member States could have on the level playing field and spread of cyber-threats across borders.

Therefore, DIGITAL SME is glad to see that the distinctions between and requirements for "Essential Services" and "Digital Service Providers" have been removed, and further definitions have been provided for the identification of Operators of Essential Services (OES) and Digital Services Providers (DSP). **Most importantly, DIGITAL SME is pleased to see that Small and Micro Enterprises are explicitly excluded from this Directive.** The burden of compliance with European legislation is often prohibitively high for most small companies, and therefore this exemption will allow them to continue to innovate and drive Europe's digital economy forwards.

While it is likely that only a small number of the service providers excluded from the exemption (providers of electronic communications networks or of publicly available electronic communications services, trust service providers, Top-level domain name (TLD) name registries and public administration) will be considered small or micro enterprises, further clarification may be required. For instance, would a cloud service provider, if they are a small or micro enterprise, be excluded unless, e.g., they provide a cloud service for a public administration? For this reason, it is still important to ensure that sufficient support measures are available for companies that do face compliance with the Directive – particularly for small and micro enterprises.

Further to this, the provision that companies to whom the Directive applies must ensure the security of their supply chains and service providers does leave the door open to small and micro enterprises being indirectly required to comply with the Directive.

**The NIS2 Directive Review offers the opportunity to establish some missing links with other EU initiatives, in particular the Cybersecurity Act and the related cybersecurity certification schemes.** To increase the level of cybersecurity and to reach further harmonisation, there is a need to connect the NIS Directive with the Cybersecurity Act and related cybersecurity certification schemes. When the NISD was first introduced, the Cybersecurity Act was not yet implemented, and this has led to different ways of implementation at national level. The suggestion of standards related to reporting requirements is a good start, providing that adequate support is offered for companies required to implement such standards.

To reach a harmonised single market, measures and requirements should be the same across different member states, which needs to be supported by certification schemes and standards. For that purpose, the NISD could further explicitly linked to recommended standards and certifications, which are unified across the EU.

**Supply Chain Security and SMEs**

While DIGITAL SME advocates for creating a level-playing field for small and micro enterprises, which requires that they are not disproportionally affected by regulation and administration burden, it is necessary to recognise the **importance of small and micro enterprises for cybersecurity due to their role in supply chains**. This is especially important given the growing dependence on ICT systems and the internet in all sectors of the economy. In many sectors, small and micro enterprises play a crucial role in supply chains and provide technologies, services, and products to other companies.

While the **NIS2 Directive explicitly 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 cybersecure 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. The Directive requires “increased diligence” during the procurement of Managed Security Service Provider’s and that data transformation and data analytics services take ““all appropriate cybersecurity measures”. Defining appropriate cybersecurity measures can help ensure that the requirements of service providers remain proportionate.

While it is important to not overburden small and micro enterprises, if they are to be assessed for their security levels, being excluded from the scope of the Directive also

means that they may be **excluded from any support measures that would lead to increasing their level of cybersecurity and to provide support (incentives, awareness, etc.) projects and funding (vouchers, etc)**. Therefore, while high thresholds and the exclusion of small and micro enterprises are generally welcome, if the forthcoming risk assessment shows vulnerabilities or that compliance with the NISD would be beneficial, **extending the coverage of the Directive may be beneficial to ensure that there are support measures in place, and that requirements for small and micro enterprises can be adapted for their specific circumstances**. To aid this, more information regarding both the requirements for entities affected by the Directive, and how the risk assessment will inform cybersecurity requirements, would be welcome.

**Reporting Thresholds and Requirements**

While the promotion of Standards ISO/IEC 30111 and ISO/IEC 29417 are welcome as a first step towards equal requirements across the Union, the fact remains that often, accessing international standards is often beyond the means of most small and micro enterprises, while their implementation remains opaque. DIGITAL SME is glad to see that rather than suggesting that such standards be required for reporting by entities outside of the scope of the Directive, the Commission recommends the establishment of voluntary schemes by Member States. Ensuring that these voluntary schemes are harmonised and not overly burdensome will be important for their uptake by small and micro enterprises and creating a level playing field.

Under Chapter IV, entities under the scope of the Directive are required to report any cybersecurity incident having a significant impact to the service they provide to the relevant CSIRT and competent authority within 24 hours. While it is assumed that the exemption of small and micro enterprises still applies to this requirement, **how this requirement relates to service providers and supply chains should be clarified further so that the reporting responsibilities for each type of entity are clear, and information on how to do so is easily accessible**.

In general, DIGITAL SME believes that the reporting of incidents should be encouraged as a means of levelling up European cybersecurity on a macro scale, but the requirements for doing so, thresholds for reporting and the means of reporting should be harmonised and easily accessible, so that the burden of reporting is not prohibitive nor off-putting for what is still a voluntary action.

As noted in Chapter V of the Directive, Member States are given the responsibility for allowing such voluntary reporting. Developing shared definitions of “significant incidents, cyber threats or ‘near misses’” can help maintain reporting thresholds at reasonable levels, while leveraging existing European initiatives for reporting, such as the CSIRT network or the relevant national authority. The introduction of international standards in

this case may be counterproductive if they are not already in common use by small and micro enterprises.

**Harmonisation of Certification and Standards Use**

In order to promote the harmonisation of the Digital Single Market, and ease the burdens of compliance, the NIS2 Directive represents the opportunity to promote existing standards and certification schemes. Member States will "encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems."

As mentioned above, International Standards and Certifications Schemes can often be unsuitable for use by small and micro enterprises, but promotion of their use by national authorities has benefits for European cybersecurity and for the Digital Single Market.

In order to encourage the uptake of relevant standards and certification schemes by small and micro enterprises the European Commission can follow the example of the SBS SME Guide on ISO/IEC 27001, to help small and micro enterprises implement security requirements for their needs. While the ISO/IEC 27001 has sufficient support for implementation, it is still complex and too costly for most small and micro enterprises to implement. An implementation guide such as the SBS Guide can be viewed as a 'best practice' on how standards can be adopted by small and micro enterprises.

Likewise, certification schemes can be harmonised across the European market, to ensure a level playing field and mutual levels of security. The implementation of the Cybersecurity Act (Regulation (EU) 2019/881) and the establishment of the cybersecurity certification framework for ICT products, services and processes is an opportunity to develop certification schemes that can be easily accessed and applied by small and micro enterprises and are shared by multiple Member States.

**About this paper**

This position has been drawn up based on input from DIGITAL SME's working group on cybersecurity (WG CYBER), led by Mr. Fabio Guasconi and Dr. George Sharkov, and coordinated by Ms. Annika Linck and Mr. James Philpot in consultation with DIGITAL SME's general membership.

**For further information on this position paper, please contact:**

Mr. James Philpot, Cybersecurity and Data Project Manager

E-Mail: j.philpot@digitalsme.eu

European
DIGITAL SME
Alliance

+32 2893 0235
https://digitalsme.eu
123 Rue du Commerce, 1000 Brussels, Belgium
VAT: BE0899786252
office@digitalsme.eu
EU Transparency Reg.: 082698126468-52