DIGITALEUROPE

Transposition of the EU Network and Information Security (NIS) Directive

Brussels, 5 July 2016

EXECUTIVE SUMMARY

The Council of the European Union published the final version of the Network and Information Security (NIS) Directive on 21 April 2016. While this needs to be formally signed off by the European Parliament this summer, the text itself has been agreed by the three EU institutions and is not expected to change. Member States are required to transpose it into national law within 21 months of its adoption. In order to assist this process, please find attached in the appendix best practice guidance on how to implement the aspects relevant to the technology industry and effectively enshrine the intentions of the drafters.

The EU NIS Directive is the first pan-European cybersecurity legislation and it focuses on strengthening cyber authorities at the national level, increasing coordination among them and introduces security requirements for key industry sectors.

Any national implementing legislation should not lose sight of the two main objectives of the Directive: (1) ensuring a high level cybersecurity of the country's critical infrastructures; (2) establishing an effective cooperation mechanism among EU Member States to further this objective. Resources should be first and foremost dedicated to achieving these two important objectives.

For the technology industry, the provisions relating to the so-called digital service providers (DSPs) are of particular interest. The Directive clearly states that there are fundamental differences between operators of essential services (OESs) and DSPs. Indeed, the latter are not to be considered critical infrastructure as such. As the legislation recognises, an incident impacting these digital services would account for a significantly lower level of risk to a country's economic security and public safety. Maintaining this distinction is essential in order to also effectively and efficiently deploy scarce resources of authorities that will have to supervise and enforce the rules.

As a result, we advocate close attention to the intended scope of the services in question and call on policy makers not to subject sectors other than those identified as DSPs and OESs to security requirements in national legislation.

With regard to jurisdiction, DSPs should be able to rely on the applicable law in the country of their main establishment, even in cases where competent authorities from more than one country are involved. On oversight, competent authorities should follow an ex-post approach as opposed to imposing a general obligation to supervise DSPs. Furthermore, they should focus on outcomes and maintain the distinction between OESs and DSPs by not subjecting the latter to requirements not foreseen by the Directive, such as auditing and binding instructions.

Security measures on DSPs should be different than for OESs, given the Directive's statement that these represent a significantly lower security risk. Decision makers should realise the goal of harmonisation for these services, recognise existing industry-led international standards, avoid technology mandates and respect the right of DSPs

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

enshrined in the Directive to define security measures most appropriate for their systems. Incident reporting should also be as harmonised as possible at the European level, should focus on incidents impacting the continuity of the service, respect the flexibility in timing of notification and created a trusted environment that encourages information sharing without exposing the notifying party to increased liability

The measures imposed on OESs will also impact other industries as security measures and incident reporting will flow-down in contract provisions. This is particularly true for cloud services. As a result, DSPs may indirectly be subject to the national laws of their customers and hence we have a keen interest in seeing internationally recognised security measures apply to these services. We also propose coordination and synergies as much as possible between the reporting requirements on both OESs and DSPs, given the latter are likely to be subject to double notification.

The Directive sets out the ambition to achieving a high common level of security of networks and information systems to improve the functioning of the internal market. To achieve this lofty goal, **national transpositions should focus on a risk-based, harmonised and international approach** that gives private sector actors the flexibility to adapt to an ever-changing threat landscape, allows cyber authorities to focus limited resources on the most significant challenges and recognises that the solution to a borderless problem needs to be global. We hope this guidance is a useful tool towards that end and would be delighted to answer any further questions you may have.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

Appendix: Best Practice Guidance for Implementation of the NIS Directive

1. Digital Service Providers

a) Scope

- The Directive determines that online marketplaces, online search engines and cloud computing services should be considered digital service providers (DSPs) and hence included in the scope of the Directive. While this is a minimum harmonisation Directive (Article 2), it is important to maintain consistency across the EU and hence Member States should not subject sectors other than those identified as DSPs or operators of essential services (OESs) – as defined in Article 3 - to security requirements in national legislation.

- The Directive explicitly states that hardware manufacturers and software developers are not OESs or DSPs and hence should not be covered by the national laws implementing the Directive (Recital 50).

- The Directive explicitly excludes from the scope of online marketplaces online services that act as intermediaries to the third-party services where the sales or service contract is ultimately concluded (e.g. comparison sites) (Recital 15).

- Search functions limited to the content of a specific website should not be covered as online search engines, even if they make use of an external provider (Recital 16).

- The definition of a cloud computing service under the Directive depends of computing resources being shared by multiple users (Article 4(19) and Recital 17). Given that private clouds (as opposed to public clouds) are dedicated to a single organisation, they should not be covered.

- The Directive underlines that there are fundamental differences between OESs and DSPs, which is the reason why DSPs are subject to different rules (Recital 57). Such distinction should be maintained when implementing the Directive.

b) Jurisdiction and Oversight

- Jurisdiction for DSPs should be attributed to only one Member State, where the operator has its main establishment in the EU, which in principle corresponds to the place where it has its head office in the EU (Article 18.1 and Recital 64). We contend that DSPs should make such a determination themselves and this decision only be subject to review if competent authorities dispute it in the circumstance of ex-post supervision activities.

- Where DSPs have network and information systems in countries other than the location of their main establishment, Article 17.3 envisages the competent authorities cooperate. From the DSPs point of view, however, it is important that the applicable law remains that of the country of their main establishment and that they remain responsible solely to the competent authority in that jurisdiction, which will act as their interlocutor.

- The Directive underlines that DSPs are subject to reactive ex-post supervision and hence competent authorities do not have any general obligation to supervise DSPs and should only take action when provided with evidence. (Article 17.1 and Recital 60). These provisions should be honoured when implementing the Directive.

- As opposed to OESs, in the case of DSPs authorities can only request information and require that DSPs remedy any failure. The Directive makes it clear that authorities have no auditing powers and cannot issue binding instructions. These provisions should be also respected at national level.

c) Additional Requirements

- DSPs' security and notification requirements are subject to maximum harmonisation (Article 16.10). This Article should be considered to apply to the products, services and solutions that make up their network and information systems. As a result, additional provisions, such as product testing, should not be required to the extent that the products and services are used in this context.

d) Security Measures and Standards

- The security measures for DSPs should be lighter than those for OESs. DSPs should be free to define how they do security and how they wish to ensure the protection of their network and information systems appropriate to the risks presented (Recital 49).

- The security measures should be process-oriented and focus on risk management. They should not require that ICT products be designed, developed or manufactured in a particular manner (Recital 51).

- The Directive emphasises that Member States shall not impose any further security requirements on DSPs (Article 16.10).

- Nevertheless, we expect guidelines from multiple actors. Member States will ensure that the measures outlined in the Directive are adopted (Article 16.1), they can encourage the use of standards to implement them (Article 19.1) and discuss the standards with European Standard Organisations in the Cooperation Group (Article 11.3(h)). ENISA will advise on the appropriate standards (Article 19.2) and the European Commission is charged with adopting implementing acts on the security measures (Article 16.8).

- Given this level of complication and the benefits of harmonisation, we advise that the national process should essentially defer to the implementing acts for agreeing appropriate measures, which in any case will need to be finalised within one year of the Directive's adoption. The implementing acts themselves should be without prejudice to DSPs' ability to define the security measures most appropriate for their systems.

- The Article on standards allows for European or internationally accepted standards to be referenced (Article 19.1). Given the maturity of international standards in place in this area, we recommend that where appropriate standards exist, certification against one of them (such as ISO 27001) should be sufficient to comply with the requirements.

- In any case standard certification should be optional, not mandatory. Article 19 underlines that any standard can only be "encouraged" and this should be "without imposing or discriminating in favour of the use of a particular type of technology."

e) Security Incident Reporting

- As with the security measures, multiple parties play a role in shaping incident reporting under the NIS Directive. Member States need to ensure DSPs notify those security incidents that have a significant impact on the provision of the service (which is in scope of the Directive) they provide (Article 16.3), the Cooperation Group is charged with discussing modalities for notifications (Article 11.3(m)) and the Commission with adopting implementing acts (Articles 16.8 and 9).

- Again, our recommendation is that national transpositions defer the process to the implementing acts, of which the implementing act on threshold for notification must be adopted within a year of the finalisation of the Directive.

- In terms of what types of incident should be reported, DSPs are charged with notifying "any incident having a substantial impact on the provision of [their] service" (Article 16.3). As for the implementation of the equivalent provisions for telecom operators under Article 13a of the Framework Directive, we believe this should be interpreted to focus on **continuity (or availability)** of the services provided. In other words, outages which reach a particular threshold (to be determined though the implementing acts) should be reported rather than any other type of security incident. This has the advantage of focusing on the incidents most likely to impact the economy or society while minimising (though not entirely eliminating) overlap with personal data breach notification requirements stemming from the General Data Protection Regulation.

- Moreover, the reporting obligation for "Operators of Essential Services" specifies that these operators shall notify "incidents having a significant impact on the continuity of the essential services they provide" which again has a clear focus on continuity (or availability) of service. The co-legislators agreed that the obligations on DSPs should be lighter than those OES (see Recital 49). The obligation for DSP incident reporting under NIS thus should not be broader than those for OES, in fact it should be even more narrowly tailored in terms of thresholds. This, again, highlights that incident reporting for DSPs should be limited to incidents which reach a particular threshold and **affect the continuity/availability of service** and not incidents relating to integrity or confidentiality of data which to a large extent is already covered by related notification requirements under the GDPR and eIDAS regulations.

- In relation to timing of notification, we appreciate the flexibility implied by the language on reporting "without undue delay" (Article 16.3). Implementation should not lead to hard deadlines as incidents vary significantly in their complexity. Uniform reporting times would lead to inaccurate reporting where the initial scope of affected systems is unclear and would impact the ability of incident response professionals to prioritise responding to the incident as opposed to reporting on it.

- As discussed, security incidents to be notified under the Directive may also require notification under data protection law, depending on whether personal data is breached. Not only does this mean reporting the same incident to different authorities, but these authorities may even be in different Member States

depending on the jurisdiction applicable to the DSP under the two laws. We recommend that Member States recognise the need and strive to provide for single notification of incidents and seek to create communication channels to share relevant information among them, without prejudice to business confidentiality.

- Competent authorities should take into account reputational and commercial implications for DSPs before sharing information about incidents publicly. More importantly, disclosing the incident could amplify the security risk. Therefore, it is important to coordinate with the actors in question before any disclosure.

- The Directive emphasises that information that is considered confidential should be treated as such (Recitals 41, 59, Article 1.5).

- Article 16.3 underlines that notification of security incident shall not expose the notifying party to increased liability.

2. Essential Operators

a) Flow Down on Security Measures

- DSPs who have OESs as customers will be subject to applicable security measures flowing down in contractual negotiations from the statutory obligations on essential operators (Article 14.1). As such, they may indirectly be subject to the national law of their customers, irrespective of the law applicable in the country of their European headquarters.

- As a result, efforts to harmonise security measures on essential operators would be welcome. While Member States have the right to impose stricter obligations on essential operators than those found under the Directive (Article 3), we recommend restraint in doing so and encourage Member States to work towards a harmonised approach. This could be achieved by avoiding additional measures in national transpositions and by seeking to determine appropriate security measures in the Cooperation Group as opposed to focusing on the national process.

- The security requirements should in as much as possible be based on international standards (such as the ISO 27x series) and recognised security best practices.

- The security measures imposed on OESs should not in any case require that particular ICT products be designed, developed or manufactured in a particular manner (Recital 51).

b) Flow Down of Security Incident Reporting

- Essential service operators are obligated to report on security incidents at their contracted DSPs that impact the continuity of their essential services (Article 16.5). DSPs will therefore be required under contract to report to the essential operator in question security incidents that might impact them.

- We appreciate the flexibility in timing of notification for OESs inherent in the phrase "without undue delay" (Article 14.3). National transpositions should not introduce specific deadlines and in any case, if OESs are asked to justify the time taken for notification, the period against which they are judged should start from when the OES is made aware of the incident, not from when DSP is aware.

- Article 14.7 envisages the Cooperation Group drawing up guidance on the circumstances for notification as opposed to the Commission's harmonising role for DSP notifications. Given the double reporting requirement for DSPs, it is important that the respective notification requirements are not contradictory and aligned as much as possible. Hence this process should be vetted against that goal. Moreover, the notification requirements for DSPs should respect the confidentiality obligations they have towards their OES customers and not ask them to share business confidential information.

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies.

DIGITALEUROPE ensures industry participation in the development and implementation of EU policies. DIGITALEUROPE's members include 62 corporate members and 37 national trade associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Ingram Micro, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies, ZTE Corporation.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: FFTI
France: AFNUM, Force Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: ICT IRELAND
Italy: ANITEC
Lithuania: INFOBALT
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK