DIGITALEUROPE

9 MAY 2022

Reporting, mandatory certification and main establishment in final NIS2 trilogues

Introduction

As trilogue negotiations for a reformed EU framework for the security of network and information systems (NIS2) are coming to an end, DIGITALEUROPE would like to take the opportunity to reiterate the digital industry's fundamental concerns around the direction of the discussions on reporting obligations, mandatory certification and main establishment.

Below, we suggest a few key amendments to the current proposals, along with their underlying justifications. We hope that despite the relative advanced status of the legislative process, our comments and suggested amendments can be taken into consideration given the importance of these topics.

Reporting obligations

Entities' resources should focus on **mitigating incidents** in the crucial phases of their emergence. The European Commission's proposal, which requires all incident notifications within 24 hours, will force entities to divert excessive resources away from mitigation towards legal compliance. This is especially true for SMEs that may fall into scope.

Alignment with the personal data breach notification regime in the General Data Protection Regulation (GDPR),[1] which sets a 72-hour deadline would have been the best way forward to ensure consistency. Absent this ideal timeline, the final text should converge around the Parliament's position, which specifies that the initial 24-hour notification should be reserved for incidents that significantly disrupt service availability, with other incidents having to be notified within 72 hours instead.

Proposed changes to Art. 20(4a):

[1] Regulation (EU) 2016/679.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

(a) ~~without undue delay and in any event within 24 hours after having become aware~~ *an initial notification of the significant incident,* ~~of the incident, an initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action;~~ *shall contain information available to the notifying entity on a best-effort basis as follows:*

(i) with regard to incidents that significantly disrupt the availability of the services provided by the entity, the CSIRT shall be notified without undue delay and in any event within 24 hours of becoming aware of the incident;

(ii) with regard to incidents that have a significant impact on the entity other than on the availability of the services provided by that entity, the CSIRT shall be notified without undue delay and in any event within 72 hours of becoming aware of the incident;

(iii) with regard to incidents that have a significant impact on the services of a trust services provider as defined in Article 3, point (19) of Regulation (EU) No 910/2014 or on the personal data maintained by that trust service provider, the CSIRT shall be notified without undue delay and in any event within 24 hours of becoming aware of the incident.

Mandatory certification

DIGITALEUROPE is concerned that with Arts 21(2)-(3), the European Commission is trying to bypass the compromise achieved on mandatory certification under Art. 56(3) of the Cybersecurity Act.[2] This article was one of the key issues debated during the Cybersecurity Act trilogues, and therefore the balance achieved there should not be so easily ignored.

The Cybersecurity Act requires the Commission to carry out a **thorough assessment of *existing* schemes** before they can be made mandatory. By contrast, under Art. 21(2) the Commission can decide to trigger mandatory schemes without any such assessment. Under Art. 21(3) the Commission, having already decided for mandatory certification without the Cybersecurity Act assessment, can subsequently request ENISA to develop a scheme if no scheme exists.

DIGITALEUROPE urges co-legislators to ensure that **certification schemes are only made mandatory after careful assessment at European level** by the European Commission following the **process established under the Cybersecurity Act**.

[2] Regulation (EU) 2019/881.

To achieve this, a **complete reference** should be made under Art. 21(2) to the assessment procedure set out under **the Cybersecurity Act's Art. 56(3)**. There is no need to repeat the elements of the assessment as they are included by virtue of the reference to another EU legal act.

Additionally, **Art. 21(3)** should be **deleted** as it should not be possible for the Commission to request the development of a new scheme purely for the purpose of making it mandatory. The Commission and Member States already have ample flexibility to request the creation of new schemes under Art. 48(2) of the Cybersecurity Act.

The Council text acknowledges the existence of the Cybersecurity Act requirements but – because of the generic way it is drafted, and because it omits elements of Art. 56(3) that are more directly linked to the assessment of schemes themselves – it might still be read as authorising the Commission to first decide for mandatory and then ask ENISA to develop the relevant scheme.

Proposed changes to Art. 21(2):

The Commission shall be empowered to adopt delegated acts*, in accordance with Article 36,* specifying which categories of essential *or important* entities shall be required to *use certain ICT products, services or processes covered by an existing European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881, or* obtain a certificate ~~*and*~~ under ~~*which specific European cybersecurity*~~ *an existing European cybersecurity* certification scheme~~s~~ *adopted* pursuant to *Article 49 of Regulation (EU) 2019/881*~~*paragraph 1*~~. The *adoption of such* delegated acts shall be ~~*adopted*~~ *preceded by an assessment of the efficiency and use of adopted European cybersecurity certification schemes* in accordance with Article ~~*35*~~6 *of Regulation (EU) 2019/881*.

Proposed changes to Art. 21(3):

Delete

Main establishment

We call upon co-legislators to provide a clear main establishment criterion under Art. 24 of the final NIS2. The original proposal as well as the Council have played with the GDPR definition of 'main establishment,' focusing on 'the place where the decisions related to the cybersecurity risk management measures are taken in the Union.' The current criterion centred around where risk management decisions are taken – let alone 'predominantly taken,' as in the Council version –

will make it too unclear for companies to know what authorities they will be supervised by.

The focus on 'decisions' ignores that the GDPR (Art. 4(16)) assumes the main establishment to be the 'place of central administration in the Union,' which can only be superseded in cases where 'decisions on the purposes and means of the processing' are taken elsewhere. This has caused a level of uncertainty around enforcement in the GDPR and is unnecessary for NIS2, where ultimately the EU headquarters will naturally be the entity that must comply. This also reflects the objective stance in the current NIS (Art. 18(1)),[3] where the focus is on the 'head office.'

DIGITALEUROPE's proposed solution to this is to either adopt the definition of **'place of central administration in the Union'** or revert back to **'head office'** as in the current NIS.

Finally, we urge co-legislators to **include number-independent interpersonal communications services (NI-ICS)** to the entities subject to main establishment under Art. 24.[4] NI-ICS are inherently cross-border in nature and their inclusion would fulfil the proposal's objective 'to ensure that such entities do not face a multitude of different legal requirements, as they provide services across borders to a particularly high extent.'[5]

Proposed changes to Art. 24(2):

For the purposes of this Directive, entities referred to in paragraph 1 shall be deemed to have their main establishment in the Union *in the place of their central administration in the Union*. ~~*the Member State where the decisions related to the cybersecurity risk management measures are taken. If such decisions are not taken in any establishment in the Union, the main establishment shall be deemed to be in the Member State where the entities have the establishment with the highest number of employees in the Union.*~~

Proposed changes to Recital 64:

In order to take account of the cross-border nature of the services and operations of DNS service providers, TLD name registries*, entities providing domain name registration services for the TLD,* content delivery network providers, cloud computing service providers, data centre service providers*, number-independent interpersonal communications services* and digital providers, only one Member State should have jurisdiction over these entities. Jurisdiction should be

[3] Directive (EU) 2016/1148.

[4] As defined in Art. 2(7), Directive (EU) 2018/1972.

[5] P. 11 of the explanatory memorandum.

attributed to the Member State in which the respective entity has its main establishment in the Union. ~~*The criterion of establishment for the purposes of this Directive implies the effective exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect. Whether this criterion is fulfilled should not depend on whether the network and information systems are physically located in a given place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not decisive criteria for determining the main establishment.*~~ The main establishment should be ~~*the place where the decisions related to the cybersecurity risk management measures are taken in the Union. This will typically correspond to*~~ the place of the companies' central administration in the Union. ~~*If such decisions are not taken in the Union, the main establishment should be deemed to be in the Member States where the entity has an establishment with the highest number of employees in the Union.*~~ Where the services are carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Director for Infrastructure, Privacy and Security Policy

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Zoey Stambolliu

Manager for Infrastructure and Security Policy

zoey.stambolliu@digitaleurope.org / +32 498 88 63 05

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 Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Assent, Atos, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Eli Lilly and Company, Epson, Ericsson, ESET, EY, Facebook, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, Johnson Controls International, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nemetschek, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: Infobalt
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK