DIGITALEUROPE

DIGITALEUROPE response to the public consultation on the draft Commission Implementing Regulation pursuant to Article 16(8) of the NIS Directive

Brussels, 19 October 2017

INTRODUCTION

DIGITALEUROPE welcomes the opportunity to comment on the draft Implementing Regulation setting out the security measures and incident reporting thresholds applicable to Digital Service Providers (DSPs) in the context of the EU's Network and Information Security Directive. DI TALEUROPE has been engaged throughout the policy development process. As previously stated, we are particularly keen to ensure that the finalised security requirements align to existing international approaches and are fully harmonised across the EU Member States, while the incident reporting thresholds should be based on information available to the DSP and be at a level that ensures only meaningful incidents are reported.

SECURITY REQUIREMENTS

As a general comment, the security requirements in many cases map to security objectives in existing, well-recognised international information security standards, which is to be welcomed. That said, it would have been helpful to more directly draw on the work of ENISA in its Technical Guidelines for the implementation of minimum security requirements for Digital Service Providers, published in February 2017. Of particular value was the mapping of ENISA's 27 security objectives to established information security standards (such as ISO 27001, C5 and the NIST Framework). The draft Implementing Regulation, on the other hand, simply lists the applicable security elements (Article 2); states that international, European or national standards could all be relevant (Article 2.5) and qualifies that DSPs remain free to adopt security measures they consider appropriate to the risk in order to meet the requirements (Recital 1).

We would welcome recognition in the Implementing Regulation of ENISA's mapping efforts; clarification that it is not mandatory to use standards to meet the requirements and affirmation that Member States should not provide additional details on security requirements and/or applicable standards in national law or through binding guidance over and above the Implementing Regulation. The latter point is particularly relevant to avoid a balkanisation of security requirements in law or in practice across the EU and is in line with Article 16.10 of the Directive, which requires Member States not to impose further security requirements on DSPs.

In terms of specific comments on the requirements in Article 2, it strikes us that Recital 4, in conjunction with Article 2.1b), is confusing security of supporting utilities with supply chain management. We would suggest that these are retained as separate categories or that the requirement applies to utilities alone. Under the section on incident handling in Article 2.2, point b) also calls for processes and procedures on reporting vulnerabilities in

information systems. Vulnerabilities normally refer to weaknesses in products that could be exploited to compromise their confidentiality, integrity or availability. This is not the same thing as actual incidents that impact the provision of the service in question. Vulnerability disclosure is a responsibility of hardware and software vendors and is not regulated by the Directive. As such, we suggest deletion of this reference. Under Article 2.4c) it is not immediately apparent what is meant by a process to reveal flaws in security mechanisms, involving technical processes and personnel in the operation flow. Potentially it could be describing penetration testing but reaching that conclusion involves a degree of interpretation. It would be good to either clarify or delete this provision. Finally, a number of the requirements are at the high-end of industry practices, including the numerous testing and documentation requirements. As such, they may be onerous for smaller DSPs in particular to implement and somewhat out of synch with the supposed 'light-touch' approach.

INCIDENT REPORTING

In terms of the overall scope of incident reporting, the Implementing Regulation appears to go beyond the intention of the policy makers who adopted the NIS Directive. Specifically, in Article 16.2, when describing the incidents DSPs are expected to adopt measures to protect themselves against the end goal is continuity of their service. This aligns closely to incidents impacting the availability of the service, as opposed to additional goals relating to the confidentiality and integrity/ authenticity of the service. As such, we would suggest that a narrower scope in Articles 3 and 4 would be appropriate.

For the adopted format of the Regulation, it is not clear what advantage is bestowed by separating Articles 3 and 4. This is especially true as the definition of parameters in Article 3 does not precisely map to the specific thresholds in Article 4. As such, we presume that the thresholds in Article 4 are the active provisions in determining the substantiality of an incident.

A key issue in making the parameters and associated thresholds usable for DSPs investigating an incident is whether they have the relevant information to hand. Article 16.4 of the Directive states that the obligation to notify an incident only applies where the DSP has access to the information needed to assess the impact of an incident against the parameters determining its significance. This is difficult to achieve at any nuanced level for economic and social impact (Article 3.5), public safety (Article 4.1c)) and material damage (Article 4.1d)). In terms of public safety (which is itself an undefined term), business-to-business (B2B) providers will likely at most be able to tell merely if a customer from a critical infrastructure or public sector has been impacted, and then perhaps only due to self-reporting by the customer. Business-to-consumer (B2C) providers will likely have even less visibility as their customers are more often than not self-serving as opposed to having a negotiated contractual arrangement. In terms of material damage, it is again the customer who will likely have the requisite information. A B2B provider may have negotiated service level agreement (SLA) terms that impose penalties depending on service outages, but that is a poor substitute for actual damage.

For the chosen thresholds in Article 4, DIGITALEUROPE is particularly concerned by the requirement to report incidents impacting two or more Member States (Article 4.1e)). The nature of cloud services is to serve multiple customers, normally over a wide geographical area. As such, outside of on-premise deployments (which may themselves involve certain data being processed off-site alongside the data of many other customers), it is almost a certainty that numerous geographical locations will be impacted by an incident. Moreover, it is often the case that the impact in specific Member States is only an estimation. To the extent that incidents can be geographically located at all without customer feedback, incidents are usually assessed in relation to the coverage area of a date

centre (or data centres), which often cover large regions (e.g. EMEAR). As such, geographical spread is not a useful standalone threshold for determining whether an incident is substantial and should only be relevant if combined with other thresholds for notification. In any case, a two Member State threshold is far too low.

For the threshold that requires notification based on unavailability of a given service for 5 000 000 user hours (Article 4.1a)), we would note that for certain services, particularly search engines, this may not necessarily amount to a substantial incident. Moreover, we would request exclusion of unavailability for voluntary maintenance purposes.

In terms of defining 'user', in Article 3.1 and 4.1b) in particular, this term should relate to customers in a contractual agreement – in other words, the first layer of customers, not the end users. For many categories of DSPs and incidents this type of user is easier to identify.

One area of confusion that is not addressed in the Implementing Regulation is risk of duplicate reporting requirements when a DSP is providing services to an Operator of Essential Services (OES), in line with Article 16.5 of the Directive. As currently described, a DSP outage which only impacts an OES will have to be reported by both the OES and the DSP. We believe this duplicate reporting is unnecessary and risks creating confusion. In the B2B space, we cannot imagine a situation where a DSP would not know that it is providing a service to an OES, either because it is subject to the regulatory requirements of a specific sector or because the OES has identified a need for information to be reported to an OES regulator. If a DSP infrastructure outage has an impact beyond just an individual OES then we agree that the DSP should report the incident. Where there is clear evidence the incident meets the criticality threshold and there is no evidence the incident is covered by an existing regulator or OES provision then we accept the DSP would include this in their reporting requirements. There is a need to provide clear guidance, however, that a DSP need not make a notification where a DSP is already obliged through its services contract to report an incident to an OES customer, as the customer will already be required to make the notification.

Finally, in terms of the timeframe for notification of incidents, the Directive provides flexibility in Article 16.3 by requiring DSPs to notify incidents "without undue delay". While the draft Implementing Regulation does not address this timeframe, we are concerned that a variety of specific time windows may be adopted at the Member State level. At least one Member State has raised the possibility of a 72-hour timeframe – which is in line with the General Data Protection Regulation's timeframe for notification of personal data breaches. Note also that guidelines for the sector-specific Payment Services Directive 2 (2015/2366) suggest that security incidents in that sector should be as little as four hours. We would welcome clarification, however, that it is not appropriate to set any specific deadline for notification in the context of the NIS Directive. This is because the appropriate timeframe for notification of an incident relating to confidentiality, integrity or availability can vary significantly. An outage impacting the availability of a service, for example, may be quickly identified and reported in some circumstances, whereas an incident stemming from an Advanced Persistent Threat that impacts integrity or confidentiality over an extended period of time (often months to years) and with a high degree of sophistication is unlikely to be as easy to unpack.

COMPETENT AUTHORITIES AND SHARING OF INFORMATION

An explicit provision should be included in the Implementing Regulation that makes it clear that DSPs need notify only once, to a single competent authority as determined by the jurisdiction provisions in Article 18.1 of the Directive. It should be clear that an incident need not be reported multiple times in multiple Member States.

Moreover, additional guidance should be provided on the requirement in Article 16.6 of the Directive that when information on incidents is shared with additional authorities, CSIRTs and single points of contacts. Any information provided as part of a disclosure must be shared with security in mind and with appropriate protections in place. Data loss by regulators is a real threat as evidenced by the recent example of a cyber breach at the Securities and Exchange Commission. Governments need to be clear where the information being reported by DSPs will be used, and shared further. This should include rules and indemnifications.

COMPATIBILITY WITH OTHER INSTRUMENTS

We call on the Commission to pay close attention to the implementation of the security and incident reporting requirements under Article 40 of the draft Electronic Communications Code (ECC) Directive. Cloud-based communication services, which since the adoption of the NIS Directive have been preparing to implement the DSP security requirements, find themselves likely to be redefined as falling under the scope of the ECC Directive once it is adopted. Ideally, we would like to see all cloud services remain under the scope of the NIS Directive. In the event that there is no change in the current course, however, we have specific concerns that we would like to raise.

The provisions under Article 40 of the aforementioned Code closely mirror requirements under Article 16 of the NIS Directive. DIGITALEUROPE calls on the Commission, however, to ensure that the eventual Delegated Acts envisaged under Article 40.5 do not diverge from the security requirements for DSPs, in order to ensure orderly compliance for such services. We are also concerned that Article 40 of the draft Code fails to allow for European harmonisation of the incident reporting requirements and allows Member States to gold plate the security requirements for communication services with national provisions. As such, we urge the Commission to work closely with Member States and ENISA to avoid divergent approaches at the national level.

--

For more information please contact:
Ramus Theede, DIGITALEUROPE's Policy Director
+45 29 90 80 30 or rasmus.theede@digitaleurope.org

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 in total 25,000 ICT Companies in Europe represented by 61 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

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

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Force Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: TECHNOLOGY 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