Responsible Vulnerability Disclosure under the NIS 2.0 Proposal

by **Sandra Schmitz and Stefan Schiffner**[*]

Abstract: Both, the NIS Directive and the GDPR introduce breach reporting obligations. In particular, in the case of the GDPR this might include an obligation to go public about an incident. These legal obligations might be in conflict with good/common practice of responsible vulnerability disclosure. This paper briefly outlines reporting duties under NISD and GDPR and maps these to hypothetical scenarios where informing end users about cyber incidents might lead to uncontrolled vulnerability disclosure. In that view, this paper analyses whether the latest proposal for a NIS Directive 2.0 strikes the right balance between the need for swift reporting and the need to investigate a vulnerability when introducing a 'coordinated vulnerability disclosure'.

Keywords: Cybersecurity; NIS Directive; GDPR; Vulnerability; Disclosure

Recommended citation: Sandra Schmitz and Stefan Schiffner, Responsible Vulnerability Disclosure under the NIS 2.0 Proposal, 12 (2021) JIPITEC 447 para 1

A. Introduction

1 A central element of EU cybersecurity legislation is the reporting of security breaches.[1] In this line, the General Data Protection Regulation (GDPR)[2] introduced reporting obligations for data controllers based on the assumption that security challenges and relevant mitigation measures can be better identified if data breaches are communicated to public authorities. Similarly, the first horizontal cybersecurity instrument, the NIS Directive (NISD)[3], introduced reporting obligations for operators of essential services (OESs) and digital service providers (DSPs) under its scope. While it may seem that the reporting obligations are a mere duplication of legal obligations, tempting entities to report only to one authority, the obligations co-exist without prejudice. Accordingly, one incident may be reported to two separate regulators under different reporting schemes and notably with different objectives (GDPR: protection of personal data; NISD: protection of underlying infrastructure). Though such double reporting is not restricted to the NISD and GDPR, the example of these two instruments perfectly highlights one potentially 'dangerous' con-

[*] SnT, University of Luxembourg, sandra.schmitz@uni.lu; stefan.schiffner@uni.lu.

[1] NIS Cooperation Group, *Annual Report NIS Directive Incidents 2019* (Publication 03/2020) 2.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/ 1.

[3] 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 [2016] OJ L 194/1.

sequence: early public disclosure of a vulnerability that challenges the effectiveness of the incident response.[4] In December 2020, the European Commission published a proposal for a new NIS Directive ('NIS 2.0 proposal')[5], which inter alia introduces a so called 'coordinated vulnerability disclosure' and addresses the need to balance swift reporting and in-depth analysis of vulnerabilities.

2 This paper briefly outlines the reporting schemes under the NISD and GDPR before the flaws of existing legislation in relation to controlled vulnerability disclosure are analysed. We will then critically evaluate how the NIS 2.0 proposal addresses the identified concerns.

B. EU Incident Reporting Schemes

3 Incident reporting obligations are not restricted to the NISD and GDPR. A number of further legal instruments also require the reporting of security incidents, such as: Directive (EU) 2018/1972 (EECC)[6], Regulation (EU) No 910/2014 (eIDAS Regulation)[7], Directive (EU) 2015/2366 (PSD2 Directive)[8]. While the NISD introduces a cross-sectoral cybersecurity incident reporting scheme, the aforementioned instruments have a limited, sectoral scope of application. Simplified, they provide for an obligation to notify (security) incidents having an actual adverse effect[9] on the security of network and information systems of essential services or digital services (NISD), electronic communications networks or services (EECC), trust services (eIDAS Regulation), and payment-related services (PSD2). The common aim is to understand (cyber-)security threats and identify vulnerabilities. In terms of simplification, we focus on incident reporting under NISD and GDPR, since the mandatory public disclosure of certain data breaches under GDPR challenges the effectiveness of a NIS incident response in general.

I. Incident Reporting under the NIS Directive

4 The NISD establishes an incident reporting framework covering the notification of significant incidents as well as requiring the implementation of security measures. As regards the obligation to report an incident, i.e. "any event having an actual adverse effect on the security of" NIS[10], the NISD differentiates between operators of essential services (OESs)[11] and digital service providers (DSPs)[12]. Member States shall ensure that OESs and DSPs notify, "without undue delay", the National Competent Authority (NCA)[13] or the computer security incident

[4] See S Schmitz and S Schiffner, 'Don't tell them now (or at all)-End user notification duties under NIS Directive and GDPR' (2021) 35:2 International Review of Law, Computers & Technology 101-115.

[5] European Commission, 'Proposal for a Directive of the European Parliament and of the Council on measure for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148' COM(2020) 823 final.

[6] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code [2018] OJ L 321/36.

[7] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L 257/73.

[8] Directive (EU) of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L 337/35.

[9] The definitions of 'incidents' vary slightly, and the PSD2 distinguishes between security incidents (as malicious actions) and operational incidents.

[10] Art 4(7) NISD.

[11] An OES is a public or private entity within one of the sectors enlisted in Annex II, which meets the criteria laid down in art. 5(2) NISD. These criteria are inter alia whether the entity provides a service that is essential for the maintenance of critical societal and/or economic activities, and an incident would have significant disruptive effects on the provision of that service. This resembles the definition of "critical infrastructure" in Art. 2(1) ECI Directive (Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [2008] OJ L 345/75) with the difference that only entities depending on NIS may qualify as OESs, and thus fall within the scope of the NISD. Member States are tasked with the identification of OES on a national basis.

[12] Annex III to the NISD lists as DSPs within the scope of the NISD only three types of services: online marketplaces, online search engines, and cloud computing services. Providers of digital services have to self-determine whether they o er services of a type listed in Annex III of the NISD in order to fall within the scope of application.

[13] The NISD provides for great flexibility either to implement a centralised or decentralised approach for designation of

response team (CSIRT)[14] of incidents having a significant impact on the continuity of the essential services they provide (in case of an OES), or incidents having a substantial impact on the provision of a digital service (in case of a DSP).[15] The NISD does not foresee mandatory notification of the individuals concerned by a security incident.[16] After consultation with the notifying entity, the NCA or the CSIRT may inform the public about individual incidents where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident, or in the case of a DSP disclosure of the incident that is otherwise in the public interest.[17] As the NISD is a Directive, results that must be achieved are laid down, but Member States are free to decide how to achieve these aims. The amount of leeway as to the exact rules to be adopted may result in varying determination of what constitutes a "significant impact" or "undue delay". Notification requirements may not only vary depending on the Member State but also within sectors. Only with regard to DSPs, the determination of substantial impact has been harmonised by Commission Implementing Regulation (EU) 2018/151[18], which specifies the relevant factors to be taken into account.[19] The different level of harmonisation for treatment of OESs and DSPs is directly linked to the different services provided (with OES directly linked to physical infrastructure) and also respects that Member States are tasked with the identification of national OES.[20] Supervision of OESs and DSPs at national level may be centralised[21] or decentralised[22], resulting in a variety of National Competent Authorities (NCAs).

II. Data Breach Reporting under the GDPR

5 Articles 33 and 34 GDPR require data controllers to notify a personal data breach to the supervisory authority, i.e. the Data Protection Authority (DPA), within 72 hours after becoming aware of it and communicate the personal data breach to the data subject without undue delay. As a 'Regulation', the GDPR has binding legal force throughout every Member State and is directly applicable. The GDPR defines a 'personal data breach' as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".[23] Reporting of data breaches to the competent DPA is not necessary where the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.[24] The same applies where the controller has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise.[25] Where notification of the DPA cannot be achieved within 72 hrs, information may be provided in phases without undue further delay.[26] In contrast to the NISD, data controllers must also communicate a breach to the

competences at national level: A slight majority of Member States opted to designate a single NCA, others designated several sectoral NCAs. Spain, for instance, employs a decentralised approach where the competent authority de-pends on whether the operator concerned is an OES or DSP); the same applies to the UK, where the NCA for OESs further depends on the sector concerned.

[14] According to art. 9 NISD, Member States shall designate one or more CSIRTs, which may be established within a NCA and must be responsible for risk and incident handling.

[15] See art 14(3) NISD as regards OES, and art 16(3) as regards DSP.

[16] Arts 14(6) and 16(6) NISD.

[17] Ibid.

[18] Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact [2018] OJ L26/48.

[19] An incident is to be considered substantial if e.g. more than 100,000 users have been affected or the damage caused exceeds EUR 1,000,000, see art 4 Commission Implementing Regulation (EU) 2018/151.

[20] Cf. Recital 57 NISD.

[21] Member States that applied a centralised approach are inter alia: Austria, Belgium, France, and Germany.

[22] Member States that applied a decentralised approach are inter alia: Czechia, Luxembourg, the Netherlands, and Poland.

[23] Art 4(12) GDPR.

[24] Art 33(1) GDPR. The exemption from the general reporting duty requires a predictive risk assessment from the perspective of an objective bystander, see Maria Wilhelm, 'Art. 33, marginal no. 9' in: Gernot Sydow (ed), *Europäische Datenschutzgrundverordnung, Handkommentar* (2nd edn, Nomos 2018). On conditions where notification is not required cf. Article 29 Working Party, *Guidelines on Personal Data Breach Notification under Regulation 2016/679 (wp250rev.01)* (2018) 18 et seq.

[25] Art 34(3)(b) GDPR.

[26] Art 33(4) GDPR.

affected individual without undue delay if there is a 'high risk' for the rights and freedoms of the affected individual.[27] This notice allows the controller to inform about the risks and advise individuals on how to protect themselves from the potential consequences of the breach.[28] Where direct communication to the individuals concerned would involve disproportionate effort, Article 34(3)(c) GDPR permits public communication. No guidance is provided as to when a delay is 'undue'; Recital 86 refers to "as soon as reasonably feasible". From a privacy perspective, this may be as soon as the data controller has determined that the prerequisites for notification foreseen in Article 34 GDPR are fulfilled. Since recital 86 also appeals for "close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities", the determination of 'undue delay' depends as well on the guidance provided by the national authorities involved.[29]

III. Interplay of the Reporting Schemes and the Potential Risk of Early Vulnerability

6 A *lex specialis* provision within the NISD foresees that where a sector-specific union act foresees security or notification requirements of at least equivalent effect, these provisions shall prevail.[30] The same applies regarding pre-existing sector-specific legislation, namely, the reporting schemes of the Telecoms Framework (now: EECC) and the eIDAS Regulation.

7 The GDPR does not constitute a *lex specialis* to the NISD as it does not regulate the notification of a significant disruption to the provision of NIS but introduces a notification obligation where personal data is at stake. Breaches of personal data are problems in and of themselves, but a breach may indicate a vulnerability in the underlying security regime.[31] Thus, although the notification obligations are very similar, they are no duplications, and do not exclude one another.[32] While from a legal perspective, it is possible to differentiate between incidents falling under the GDPR and such falling under the NISD, in practice, most security incidents will involve some sort of personal data, meaning that the data controller will have to report these incidents to the NISD NCA and the DPA. Cooperation of these authorities in the sense of co-ordination and information-sharing is only recommended under the NISD and the GDPR framework ('should'/'shall' cooperate) when dealing with an incident/data breach. They operate independently. The lack of formal cooperation may result in different advice by the NIS NCA and competent DPA to the reporting entity surrounding public disclosure of an incident. From a privacy perspective, the DPA may request instant information of the data subjects concerned, although the entity concerned has a basic interest in delaying notification to investigate an attack. In terms of delaying notification of the data subject, recital 86 GDPR requires that guidance be respected when provided by the DPA or by other relevant authorities such as law-enforcement authorities. This may suggest that guidance by a NIS NCA to delay going public may justify a delay in notifying data subjects. However, since the operative provisions of the GDPR do not require cooperation and information-sharing by the DPAs and NIS NCAs, the initiation of such cooperation may in the worst case lay at the hand of the reporting entity. The fact that cooperation is only mentioned in a recital requires to recall the nature of recitals: The recitals of an EU legal act are not in themselves legally binding in the same way that the operative articles are. In principle, recitals "state concisely the reasons for the main provisions of the enacting terms of the act".[33] The function of recitals as an interpretative legal tool has been developed in the case law of the CJEU to resolve ambiguities where an operative provision is not clear[34] or to help to explain the purpose and intent behind a normative instrument.[35] Obviously, recital 86 goes further than explaining purpose or intent, or the reasons for Article 34 GDPR, when it appeals for "close cooperation with" authorities when determining the lawfulness of a deviation from the

[27] Art 34 GDPR; see also Recital 86. On how to assess risk and high risk see Article 29 Working Part (n 24) 22 et seq.

[28] Recital 86.

[29] Mario Martini, 'Art. 34 DS-GVO, marginal no. 44' in B Paal and D Pauly (eds), *Beck'sche Kompakt-Kommentare, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz* (2rd ed Beck 2021).

[30] Art. 1(7) NISD.

[31] European Data Protection Board, *Guidelines 01/2021 on Examples regarding Data Breach Notification* (Version 1.0, 2021) 6.

[32] Cf. Art. 1(3) NISD.

[33] European Union, *Joint Practical Guide of the European Parliament, the Council and the Commission for Persons Involved in the Drafting of European Union Legislation* (2nd ed Publications Office of the European Union 2015) 32. By stating the reasons on which a legal act is based, recitals give effect to Art. 296 TFEU.

[34] See T Klimas and J Vaiciukaite, 'The Law of Recitals in European Community Legislation' [2008] ILSA Journal of International & Comparative Law 61, 86 with further references.

[35] Cf. case C-173/99 *BECTU* EU:C:2001:356, paras. 37-39.

obligation to inform "without undue delay". Other than the operative provisions of the GDPR, recital 86 further recognises that "the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication". Considering that early disclosure of an incident may interfere with the containment and recovery of an incident, it seems that the GDPR recognises this risk as a reason for delay. When the recital uses the notion 'may' instead of 'must' in relation to the justification for more time, it remains unclear which "need to implement appropriate measures against continuing or similar breaches" justifies a delay.[36] Also, the justification seems to be restricted to an ongoing attack (and 'similar breaches'), which leads to the further question as to when an attack is still ongoing. An attack may be terminated, but the fixture of a vulnerability may be ongoing. Therefore, an entity may have a keen interest in further delaying the notification of data subjects opposed to what the GDPR requires. Considering that there are also scenarios, where the same incident is notified by two different entities to two different authorities (for instance where a DSP reports an incident to the NIS NCA, and the data controller (using a service provided by the DSP) to the competent DPA under the GDPR), there is a likelihood that an early disclosure to the public by the data controller hampers the incident response of the DSP. Instead of specifying when delay is not 'undue', the legislator limits its focus on legitimate suspension of notification in the following recitals on law enforcement interests. Accordingly, recital 88 GDPR sets forth that in setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, such rules and procedures should "take into account the legitimate interests of law enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach". In that line, the guidance on personal data breach notification issued by the Article 29 WP[37] solely addresses interests of law enforcement authorities as justifying delay. Consequently, early disclosure is primarily considered as potentially hampering criminal investigations. As of date, little attention is paid to the interests of the entity encountering a security incident. One reason for this may be the fact, that national case law in which fines have been imposed upon data controllers primarily relate to failures in implementing technical and organisational measures to ensure secure processing, right to access or right to erasure.[38] Many of the cases outlined in the EDPB 2019 annual report highlighted a lack of proper technical and organisational measures for ensuring data protection that resulted in data breaches without an outside attack.[39]

8 The question remains as to which legal consequences a data controller faces when—in order to not hamper their containment and recovery strategy—they delay notification of data subjects concerned of a data breach. Pursuant to Art. 82 (1) GDPR, they will be liable for the damage caused by the suspended or delayed notification of the subject.[40] Accordingly, this liability is limited to damage that occurs from the point of time where a delay is considered undue. The DPA may use its investigative and corrective powers (Article 58 GDPR), and, once an infringement of the obligation under Article 34 GDPR is established, may issue an administrative fine of up to EUR 10 million, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.[41] When deciding whether to impose an administrative fine and deciding on the amount of the fine due regard has to be given to a number of factors enshrined in Article 83 (2) GDPR. These factors include inter alia actions taken to mitigate the damage suffered by data subjects (lit. c), the degree of cooperation with the supervisory authority to remedy the infringement and mitigate the possible adverse effects of the infringement (lit. f), and to what extent the controller notified the infringement to the controller (lit. h). Article 83 (2) GDPR also provides for a catch-all element when "any other mitigating factor" needs to be taken into consideration, which must—in light of the aforementioned factors—also include the containment and recovery of an incident to identify an attacker, vulnerability or certain modus operandi. It remains to be seen how much weight national DPAs attribute to an effective NIS response—either

[36] The same applies to the questions which law enforcement interests may justify a delay, however, law enforcement authorities are more likely to provide guidance. There is a clear need to concretise justifications from the side of DPAs, see Mario Martini, 'Art. 34 DS-GVO, marginal no. 45' in B Paal and D Pauly (eds), *Beck'sche Kompakt-Kommentare, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz* (2rd ed Beck 2021).

[37] Article 29 Working Party (n 24) 1.

[38] Confer chapter 6 on supervisory authority activities in 2019 in European Data Protection Board, *2019 Annual Report, Working Together for Stronger Rights* (2020).

[39] Ibid.

[40] Mario Martini, 'Art. 34 DS-GVO, marginal no. 7' in B Paal and D Pauly (eds), *Beck'sche Kompakt-Kommentare, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz* (2rd ed Beck 2021). This view is not undisputed: according to *Reif* (Yvette Reif, 'Art. 34 DS-GVO, marginal no. 18' in Peter Gola (ed), *DS-GVO, Datenschutz-Grundverordnung VO (EU) 2016/679, Kommentar* (2nd ed Beck 2018)) a suspended or delayed notification only triggers claims for damages under general tort law.

[41] Art. 82 (4) lit a GDPR.

as a justification or at least as an important factor when deciding upon and setting the amount of a fine.

IV. Interim Summary

9 At a first glance, the aforementioned lack of mandatory cooperation may account for an early incident disclosure. Where the DPA treats an incident independently from the NIS NCA, privacy may prevail over an investigation into the roots and causes of an incident from a technical perspective. As DPAs advise on when data subjects should be notified, an entity may feel obliged to disclose an incident instantly, whereas from a cybersecurity perspective delay is required. This theoretical risk is rooted in the different aims of the legal instruments. The GDPR concerns the protection of personal data and publicity of a data breach should put the data subjects concerned in a position to mitigate immediate risks of damage. Guidance on data breach notification by the EDPB European Data Protection Board[42] thus solely focuses on the data protection position and addresses issues in relation to the timing of notification from a mere privacy viewpoint. Other than protecting the rights and freedoms of a natural person, publicity of incidents under the NISD aims at (re-)establishing information security, i.e. confidentiality, integrity and availability of NIS. As a consequence, the individual affected by a mere security incident may only be informed of the incident, where public awareness is necessary in order to prevent an incident, to deal with an ongoing incident, or limited to DSPs, disclosure is in the public interest.[43] Recital 86 GDPR addresses the dilemma of early disclosure by recognising that "the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication". The wording of the justification suggests that it should be limited to continuing and ongoing data breaches; it does not encompass ongoing security incidents as such. Hence, it would for instance fall short in an incident which incidentally compromised consumer data, but leads to an ongoing attack targeted at other vital systems of the OES or DSP.[44] However, since the justification is 'only' part of the recital, this supports the interpretation of 'undue delay' in the operating provision, but does not provide legally binding limits to the scope of Article 34 GDPR. Also, mitigation of an incident and an effective NIS response are factors to be considered when deciding upon the imposition of an administrative fine for infringing Article 34 GDPR.

C. Responsible Disclosure

10 In the light of the above, the following section analyses two relevant examples discussed by the EDPB in its guidelines 01/2021[45] with regard to their potential for harm in the case of premature public incident disclosure. As aforementioned, legal reporting duties, in particular public disclosure, might conflict with the professional ethical standards of IT-Security staff. However, this conflict might appear larger than it is due to a general overestimation of what can be learned from reporting an incident about the mechanics of a vulnerability.

11 **Incidents aren't Vulnerabilities – Definitions.** A vulnerability is a set of conditions that allows the violation of a security (or privacy) policy. Such conditions might be created by software flaws, configuration mistakes and other human errors of operators, or unexpected conditions of the environment a system runs in. Exploits are software that exploit vulnerabilities for some effect (even be it only to demonstrate the existence of vulnerabilities). Malware is some software that is designed with malicious intent. It might or might not make use of exploits or vulnerabilities. An incident from a technical perspective is any successful or attempted violation of a security or privacy policy. It might involve vulnerabilities, exploits malware, or none of these concepts.[46] Lastly, a patch is a piece of software that is designed to improve an IT system by modifying its software or data.

12 **Controlled (or Responsible) Vulnerability Disclosure** is a process that allows IT vendors and finders of vulnerabilities to cooperatively find solutions that reduce the risk associated with public vulnerabilities;[47] I.e., a researcher (finder) who discovered a flaw in a system, informs the developer (vendors, providers) of a system about a flaw and potential fixes. This allows the developer to take mitigation measures (patches, traffic monitoring, blocking) to eliminate or reduce the risk that the vulnerability is used by an attacker. Only then the vulnerability is published. Controlled vulnerability

[42] European Data Protection Board (n 31), or Article 29 Working Party, (n 24).

[43] cf. Articles 14(6) and 16(7) NISD.

[44] Schmitz and Schiffner (n 4) 110.

[45] European Data Protection Board (n 31).

[46] Allen D Householder et al, 'The CERT ® Guide to Coordinated Vulnerability Disclosure' [2017] (August) Technical Report Cmu/Sei-2017-Sr-022 <https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf> last accessed 26 August 2021.

[47] Cf. ISO/IEC 29147.

disclosure is detailing out this process, in particular how to act if developers are not willing or not able to react accordingly. This type of disclosure may eventually result in the suspension of going public about an incident in order to elaborate the appropriate containment strategy including vulnerability fixtures.

I. Case Analysis.

13 In its Guidelines 01/2021 the EDPB outlines 18 fictional cases that shall support and guide data controllers and processors to better understand reporting obligations under the GDPR. Two of these exemplary cases will be analysed that demonstrate risks of being in conflict with general controlled vulnerability disclosure guidelines. Due to the sample cases being of a very general nature, further details have been added by the authors to highlight potential conflicts.

14 Since the issue of hampering investigations by early disclosure in particular arises in ransomware and data exfiltration attacks, the subsequent analysis focuses on these attacks. Attacks of this kind are largely based on software vulnerabilities as opposed to human error, natural disaster or traditional crime.

15 **Ransomware Attacks.** Ransomware is a type of malware attack which attacks the availability of data of the victim in order to extort money from the victim.

16 EDPB Case no. 03: “The information system of a hospital/healthcare centre was exposed to a ransomware attack and a significant proportion of its data was encrypted by the attacker. The company is using the expertise of an external cybersecurity company to monitor their network. Logs tracing all data flows leaving the company (including outbound email) are available. After analysing the logs and the data the other detection systems have collected the internal investigation aided by the cybersecurity company determined that the perpetrator only encrypted the data without exfiltrating it. The logs show no outward data flow in the timeframe of the attack. The personal data affected by the breach relates to the employees and patients, which represented thousands of individuals. Backups were available in an electronic form. Most of the data was restored but this operation lasted 2 working days and led to major delays in treating the patients with surgery cancelled / postponed, and to a lowering the level of service due to the unavailability of the systems.” The EDPB concludes that this sort of attack might lead to reporting obligations to the general public if a sever interruption of the service for many customers is observed and the involved data amounts to special categories of data.[48]

17 The case seems to be inspired by a Ransomware attack which largely effected the NHS[49] in 2017.[50] It needs to be pointed out that the malware WannaCry[51] was epidemic. Hence, it was most likely not targeted at the NHS as such. Its large spread was possible since it was based on the so called EternalBlue exploit which made use of the vulnerability CVE-2017-014.[52] This exploit targeted a certain implementation of Microsoft’s smb protocol.[53] Although a related vulnerability a patch was available, many systems remained unpatched.[54]

18 Beside the direct effect of the attack, the large spread of the malware also demonstrated the vast number of unpatched systems and in particular the vast number of systems which are likely hard to patch due to legacy system support. In such a case, one might advise against informing the general public immediately to avoid copycat attacks.[55] In simple terms, publicity should be avoided until a patch for

[48] ibid.

[49] UK national health service (https://www.nhs.uk).

[50] Acronis iGmbH, ‘Case study the NHS cyber attack’ (Acronis) <https://www.acronis.com/en-us/articles/nhs-cyber-attack/> last accessed 26 August 2021.

[51] Kaspersky, ‘What is WannaCry ransomware?’ (Kaspersky Resource Center) <https://www.kaspersky.com/resource-center/threats/ransomware-wannacry> last accessed 26 August 2021.

[52] For more on the vulnerability, see National Cybersecurity FFRDC, CVE-2017-0144m (Mitre Corporation) <https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-0144> last accessed 26 August 2021.

[53] For more on the current revision and previous versions of the Microsoft server message block (SMB) protocol, see Microsoft, ‘Server Message Block (SMB) Protocol’ (Microsoft) <https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-smb/f210069c-7086-4dc2-885e-861d837df688> last accessed 26 August 2021.

[54] It has to be noted that not patching is not always neglect: often systems in production stay unpatched for longer since system owners need time to investigate if the patch is compatible with specialised equipment.

[55] A delay needs to consider that due to high impact of some observed infections, controlled disclosure may not even be possible.

the software vulnerability is released in order to prevent further personal data to be interfered with.

19 In contrast to this, is EDPB Case no. 04: “The server of a public transportation company was exposed to a ransomware attack and its data was encrypted. According to the findings of the internal investigation the perpetrator not only encrypted the data, but also exfiltrated it. The type of breached data was the personal data of clients and employees, and of the several thousand people using the services of the company (e.g., buying tickets online). Beyond basic identity data, identity card numbers and financial data such as credit card details are involved in the breach. A backup database existed, but it was also encrypted by the attacker.”

20 Assuming, contra to Case no. 3, that no public knowledge of the mechanics of the attack can be derived nor was the underlying malware as widespread or at least would not expose vulnerabilities in widespread systems, informing the general public is unlikely to trigger more attacks. However, the leaked information poses high risks for the affected individuals, so it is advisable to inform victims and the public as soon as possible.

II. Protection Goal Conflict GDPR – NISD

21 Extending the EDPB’s fictional cases magnifies the root cause of the conflict among GDPR and NISD with regard to incident reporting, namely, the different protection goals. On one hand, the NISD aims at the protection of the underlying (vital) infrastructure. That is, its focus is on availability, though confidentiality and integrity might be needed to ensure the former. Further, the NISD operates under the assumption that OESs and DSPs use similar systems for their operation. That means in turn, knowledge of an incident might help to uncover ongoing incidents with other providers. Lastly, the analysis of incidents might unveil vulnerabilities that are shared with other providers. In short, incident reporting aims at the discovery of large-scale attacks and identification of underlying vulnerabilities in order to allow coordinated incidence response (short term) and an improved level of cyber security/preparedness (long term). On the other hand, the GDPR aims at the protection of users’ rights with focus on confidentiality (of the users’ data). Here, incident reporting to the DPAs has the same aims as reporting under the NISD. However, regarding the duty to inform affected users, it goes further: it shall allow users to take personal mitigation actions, e.g., changing passwords, blocking payment cards etc. and thereby, prevent the harm from materialising.

D. Vulnerability Disclosure under the NIS 2.0 Proposal

22 With the COVID-19 pandemic, the foreseen revision of the NISD gained momentum. Following an accelerated review of the NISD, the European Commission adopted a proposal for a revised NISD on 16 December 2020 (‘Proposal for NIS 2.0’)[56], although the first report of the Directive was only due in May 2021. This clearly shows the commitment of the European Commission to increase cyber resilience. While the NISD set up cooperation mechanisms between Member States, the NIS 2.0 proposal aims to strengthen and extend cooperation, as well as exploit synergies.

I. The Operative Provisions on Coordinated Vulnerability Disclosure and Cooperation Mechanisms in the NIS 2.0 Proposal

23 Remedying the causes of NIS vulnerabilities is identified as an important factor in reducing cybersecurity risks. The proposal recognises that the reporting entities are often third parties relying on a particular ICT product or service, and thus, the manufacturer or provider of ICT products or services should also receive vulnerability information. In that regard, the NIS 2.0 proposal introduces a framework for coordinated vulnerability disclosure[57] and requires Member States to designate CSIRTs to act as trusted intermediaries and facilitate the interaction between the reporting entities and the manufacturers or providers of ICT products and services.[58] Coordinated vulnerability disclosure, as described in the proposal, specifies a structured process through which vulnerabilities are reported in a manner allowing the diagnosis and remedy of the vulnerability before vulnerable information is disclosed to third parties or to the general public. Where entities become aware of an incident, they are required to submit an initial notification without undue delay and not later than 24 hours, followed by a final report not later than one month after.[59] While the initial notification is limited to the information strictly necessary to make the competent authorities aware of the incident and allow the reporting entity to seek assistance, the final report must contain a (i)

[56] European Commission (n 5).

[57] Art 6(1) NIS 2.0 Proposal.

[58] Recital 29 NIS 2.0 Proposal.

[59] Art 20(4) NIS 2.0 Proposal.

detailed description of the incident, its severity and impact; (ii) the type of threat or root cause that likely triggered the incident; (iii) applied and ongoing mitigation measures. This two-stage approach is similar to the reporting in stages under the GDPR, where information may be provided in phases if full notification of the DPA cannot be achieved within 72 hrs.

24 The aim of the two-stage approach becomes clear in the recitals: the reporting entity's resources should not be diverted from activities related to incident handling, which should be prioritised.[60] Coordinated vulnerability disclosure also takes into account coordination between the reporting entity and the manufacturers or providers of ICT products and services as regards the timing of remediation and publication of vulnerabilities.[61] The role of the CSIRT as the coordinator in that process should include the identification and contact of further entities concerned, support of reporting entities including negotiations with regard to disclosure timelines, and the management of vulnerabilities that affect multiple organisations (so called multi-party vulnerability disclosure).[62] ENISA is required to develop and maintain a European vulnerability registry for the discovered vulnerabilities.[63] Although cooperation under the NIS 2.0 proposal is still attached to cross-border incidents, there is a clear request to strengthen information sharing of national authorities,[64] e.g. by establishing cooperation rules between the NIS NCAs and DPAs to deal with infringements related to personal data.[65] However, cooperation of NIS NCAs and DPAs as required in Article 32 NIS 2.0 Proposal focuses on NCAs notifying DPAs when they have an indication of a personal data breach infringement by important or essential services (prieviously known as OES and DSP) of the security and notification obligations enshrined in Articles 18 and 20. Since NCAs are obliged to notify indications of a personal data breach to the DPA 'within a reasonable period of time',[66] yet another timeframe is introduced, adding to the complexity of determining 'undue delay' under GDPR and suggesting that the NCA may withhold information where the data controller would be obliged to notify the DPA 'without undue delay'.[67]

II. Strengthening Coordination, but Laxity Towards Responsible Disclosure?

25 While at first glance, the introduction of a coordinated vulnerability disclosure suggests a strengthening of control in the sense of responsible disclosure—i.e. it respects the interest of an entity to delay information of the public—this may not be the case. It is merely that the Proposal lays down a two-stage approach to incident reporting to strike a balance between, on the one hand, swift reporting to NCAs that helps mitigating the potential spread of incidents and allows entities to seek support, and, on the other hand, detailed reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual companies and entire sectors.[68]

26 The clear commitment to put the incident response ahead of detailed reporting, does not eliminate the conflict with swift reporting to data subjects under GDPR since this remains predominantly an issue of GDPR compliance and does not concern obligations under the NISD. The delay granted for detailed reporting may tempt entities even more to depart from the 'without undue delay' reporting to individuals under the GDPR. The reporting in phases of a NIS incident to NIS NCAs may become the default reporting mechanism in light of prioritizing the incident response. As publicity may hamper an incident response, data controllers may give priority to the technical incident response over informing data subjects. Even when Article 20(1) and (2) NIS 2.0 Proposal introduce a GDPR-like obligation to inform service recipients of incidents that are inter alia likely to adversely affect the provision of that service 'without undue delay', the ratio of the NISD remains an effective incident response. Accordingly, this third-party notification is only required 'where appropriate', suggesting that this is only necessary where measures are available to the service recipients to mitigate the resulting risk

[60] Recital 55 NIS 2.0 Proposal.

[61] Recital 28 NIS 2.0 Proposal.

[62] Recital 29 NIS 2.0 Proposal.

[63] Art 6(2) NIS 2.0 Proposal.

[64] Art 26(1) NIS 2.0 Proposal.

[65] Recital 77 NIS 2.0 Proposal.

[66] Art. 32(1) NIS 2.0 Proposal.

[67] The EDPS suggests changing the wording of the Proposal to 'without undue delay' in order to enable DPAs to perform effectively their tasks, European Data Protection Supervisor, *Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive* (11 March 2021), 17.

[68] cf. Recital 55 NIS 2.0 Proposal.

themselves,[69] and where incident publicity does not interfere with effective incident response in a whole.

27 During the consultation process various stakeholders[70] addressed a necessity to align reporting authorities, thresholds, timeframes and penalties in EU legislation to eliminate "persisting redundancies in terms of incident reporting and double notification requirements under different legal regimes".[71] The proposal suggests that for the purposes of simplifying the reporting of security incidents, Member States should establish a single entry point for all notifications required under NISD and also under other Union law such as the GDPR.[72] Whether a single entry point may alleviate issues in relation to early disclosure to the public in form of individual data subjects remains to be seen as a single entry point does not mean that notified authorities will treat a reported incident in the same way. A single entry point for reporting to regulators is also not related to obligations to inform the public. However, there was also no necessity from the legislator to address this issue in the NIS 2.0 proposal since the risk of early disclosure is merely an issue of GDPR compliance. As long as the GDPR does not address the containment and recovery of an incident along with further interests such as law enforcement as a justification to delay notification of data subjects, the conflict persists. The sole conflict that the NIS 2.0 Proposal eliminates are the legal consequences for non-compliance under the GDPR and NIS instrument: Article 32(2) NIS 2.0 Proposal clarifies that where a DPA imposes an administrative fine, a NCA shall not impose an administrative fine for the same infringement. Again, failure to comply with notification obligations towards the regulatory authority, and failure to comply with the notification obligation towards the data subject/service recipient are different infringements. An entity that informs the DPA and NCA of a security incident involving personal data but does not inform the data subject without undue delay to deal with an incident is potentially subject to legal sanction under the GDPR.

28 In sum, the coordinated vulnerability disclosure and strengthening of cooperation do not provide a solid framework for responsible disclosure since every data controller has the sword of Damocles hanging over their head in the form of mandatory disclosure of data breaches to data subjects without undue delay.

E. Conclusion

29 Reporting obligations under NISD and GDPR are neither redundant nor conflicting at large, but stem from the different goals of the respective legislation. However, in detail, these protection goals might be conflicting, and accordingly, reporting under one instrument might undermine protection efforts under the other regime. In particular, premature notification of users (and by this the general public) might lead to adverse effects with regard to cybersecurity, i.e., the reported incident under GDPR might lead to uncontrolled vulnerability disclosure. This in turn might expose other entities and services to risks since they did not have the head start to patch vulnerabilities as they would have had under a controlled disclosure regime. It is creditable that the NISD 2.0 proposal acknowledges the concept of controlled disclosure. However, without matching obligations within the GDPR, this might cause further conflicts: the GDPR might require informing users while under the NISD 2.0 Proposal, NCAs may advice controlled disclosure, which in practice can only be effective if information is held back from the general public to allow time to patch systems. The conflict is not trivial due to protection goals that might be in competition. In order to trade off the interests of OESs, DSPs and data subjects, NCAs and DPAs need to collaborate. However, such collaboration is currently not mandatory under EU law. The conflict could also be alleviated if the normative provisions of the GDPR are aligned and provide for a precise justification for delaying information of data subjects in the case of contravening interests of law enforcement, or interests of the data controller concerned in responding adequately to the incident.

Acknowledgment

The research for this article was funded by the Luxembourg National Research Fund (FNR) C18/IS/12639666/EnCaViBS/Cole, https://www.fnr.lu/projects/the-eu-nis-directive-enhancing-cybersecurity-across-vital-business-sectors-encavibs/.

[69] Cf. Recital 52 NIS 2.0 Proposal.

[70] Inter alia Microsoft, bitkom, Digitaleurope.

[71] See e.g. Sebastian Artz, 'Position Paper "Roadmap NIS-Review Bitkom Views Concerning the Combined Evaluation Roadmap / Inception Impact Assessment' (*Bitkom*, 13 August 2020) <https://www.bitkom.org/sites/default/files/2020-08/bitkom_positionpaper_nis_roadmap_final_200813.pdf> last accessed 26 August 2021; and European Banking Authority, 'Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2)' Final Report (*EBA*, 27 July 2017) <https://www.eba.europa.eu/documents/10180/1914076/Guidelines+on+incident+reporting+under+PSD2+%28EBA-GL-2017-10%29.pdf/3902c3db-c86d-40b7-b875-dd50eec87657> last accessed 26 August 2021.

[72] Recital 56 NIS 2.0 Proposal.