Don’t tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR

Sandra Schmitz-Berndt & Stefan Schiffner

To cite this article: Sandra Schmitz-Berndt & Stefan Schiffner (2021): Don’t tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR, International Review of Law, Computers & Technology, DOI: 10.1080/13600869.2021.1885103

To link to this article: https://doi.org/10.1080/13600869.2021.1885103

© 2021 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

Published online: 11 Feb 2021.

Submit your article to this journal

Article views: 283

View related articles

View Crossmark data
Don’t tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR

Sandra Schmitz-Berndt and Stefan Schiffner
SnT, Université du Luxembourg, Esch sur Alzette, Luxembourg

ABSTRACT
In this article, we critically analyse the timeline for notifications of third parties under the NIS Directive and the GDPR in the case of security and privacy incidents from a legal and technical perspective. While a need to mitigate an immediate risk of damage for an individual would call for prompt notification of data subjects, there are scenarios which may justify a delay in communication, for instance where a service provider needs to analyse the current attack to prevent further attacks and assess the full impact. Further, we argue that notification duties in the GDPR and NISD have different protection goals which may conflict in the context of a given incident. Since they are triggered by the same incident, they may contain redundancies, which bears potential for synergies which should be capitalised by the competent authorities.

ARTICLE HISTORY
Received 29 September 2020
Accepted 7 January 2021

KEYWORDS
Computer security; IT law; privacy

Introduction
In 2016, two important legal instruments aiming to ensure an appropriate level of security for information technology (IT) and the data processed by it were passed: the General Data Protection Regulation (GDPR), and the Network and Information Systems (NIS) Directive. Although in terms of risk-based security measures, requirements in the GDPR and the NIS Directive are well aligned, the instruments have distinct protection goals; the GDPR covers privacy and data protection rights concerning personal data of individuals, while the NIS Directive encompasses the information security for infrastructures. More specifically, the focus of the former is confidentiality of data relevant to data subjects (natural persons), with integrity and availability of said data being a supporting condition for this; while in the latter, the focus is on availability of the service, with confidentiality and integrity being supporting factors. In many cases, interferences with information security also affects personal data. While the NIS Directive is broader in terms of the subject matter covered, i.e. digital data including any data relating to network and information systems and its provision and continuity, it is more restrictive in regards to its addressees, which only include identified operators of essential services (OES) and digital service providers (DSP).
Both instruments introduce similar notification obligations based on the assumption that security challenges and relevant mitigation measures can be better identified if security risks and data breaches are communicated to public authorities. As both acts are considered without prejudice, in practice, the same incident may have to be reported to two separate regulators. While at a first glance, this does not raise concerns, the issue becomes twofold where the GDPR also requires data controllers to communicate a personal data breach without undue delay to the data subject. Essentially, communication to the data subject means going public about a security incident. This poses challenges for an NIS provider who may have an interest in delaying publication of the breach.

The remainder of this article is organised as follows: First, we outline the incident notification schemes, including the timeframes for reporting as well as the duties of the regulators under NIS Directive and GDPR. Second, from an interdisciplinary perspective, we will present scenarios in which diverting from the set timeframe may be justified due to a prevailing and legitimate interest in suspending end user notifications. Taking the incidence response cycle as guide, we try to interpret the indefinite legal concept of ‘without undue delay’. In our conclusion, we will also address this issue as not only relevant with regard to the interplay between the NIS Directive and the GDPR, but also in light of a sea of sector-specific regulation encompassing similar notification obligations.

Background

**Information security vs privacy**

Information security and privacy interact in a complex fashion. One can argue that a breach in one might lead to an incident in the other field. It is obvious that unauthorised access to a database with, e.g. VISA card information, on its basis an IT-Security incident, leads to a privacy breach. The other way around might be less obvious though; personal information leaked, might be used in spear-phishing attack, e.g. the attacker might learn that a targeted person is a client of a specific bank, and use this information to formulate a more convincing spear-phishing email that can be tailored to significantly increase the likelihood that a victim is tricked into revealing sensitive information such as login details, including passwords. See Halevi, Memon and Nov (2015) for more on how personal information can be exploited for more successful phishing attacks.

So, set against this backdrop: what is the difference between privacy and security? In short, the difference is the protection goals, i.e. which assets need to be protected from whom and who are the risk bearers. Traditionally in information security, we distinguish between three dimensions: i.e. Confidentiality, Integrity, and Availability. A secure information system always requires all three dimensions to a certain extent. Moreover, to describe a protection goal for a given application, one needs to describe the stakeholders and the adversary (assumptions and capabilities).

Example I. Consider the IT security of a power plant. The plant can be controlled remotely in order to adjust its output coordinated with neighbouring plants to the market needs. An adversary might attempt to falsify messages that lead to an unwanted reduction of power production, which in turn would reduce the revenue of this plant (assuming it’s a single attack and other power providers step in to avoid a blackout). Hence, in this scenario, the operator of the plant is the main risk bearer, the main
protection goal is availability, and the main adversary is an external attack that attempts to modify messages, i.e. a breach of the messages’ integrity leads directly to an availability breach.

Example II. Consider a hotel booking platform. Users need to provide payment details as collateral for their bookings, which are stored in a database. An adversary might attempt to access this database with the aim of using this payment data for fraudulent payments. This would at first have an impact on the users of the booking service, who are the main risk bearers here. Therefore, the main protection goal is confidentiality to prevent an external attack from the abuse of personal data, e.g. in an identity theft scheme.

Hence, Confidentiality, Integrity and Availability are relevant for information security and personal data protection, though with some differences in emphasis of the dimensions. For privacy, the literature further distinguishes three more protection goals: unlinkability, transparency and intervenability (Hansen, Jensen, and Rost 2015). Here, unlinkability means that two artefacts concerning the same context, cannot be related to this context by an unauthorised party. Hence this could be seen as confidentiality of metadata; transparency requires technical measures that allow a data subject to investigate how data is processed, and intervenability measures allow subjects to change the way of processing (correct data, retract consent, etc.).

Both legal instruments, that is the GDPR and NIS Directive, reflect these protection goals with reference to the notification obligations. For the GDPR, these obligations concern mainly confidentiality and unlinkability breaches, while for the NIS Directive the main concern is disruptions of service, hence availability breaches.

**Incident handling under NIS Directive and GDPR: notification obligations**

Both instruments recognise prevention as a key element of data security. If nevertheless, a data breach/security incident occurs, a swift response is required to mitigate the risks and maintain an overall high common level of NIS security. A key element of effective risk-management under GDPR and NIS Directive is the notification of the competent authority.

**The NIS Directive incident notification scheme: notification obligation for OESs and DSPs**

As regards the obligation to report an incident (i.e. ‘any event having an actual adverse effect on the security of NIS), the NIS Directive differentiates between operators of essential services (OESs) and digital service providers (DSPs). An OES is a public or private entity within one of the sectors enlisted in Annex II, which meets the criteria laid down in Article 5(2). Member States are supposed to define essential services and identify OES within their territories. In contrast, Annex III to the NIS Directive lists as DSPs within the scope of the NIS Directive only three types of services: online marketplaces, online search engines, and cloud computing services.

Member States shall ensure that OESs and DSPs notify, ‘without undue delay,’ the national competent authority (NCA) or the computer security incident response team (CSIRT) 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).
Of relevance for this article is the timeframe within which an incident must be reported. The NIS Directive only refers to the non-concrete concept of ‘without undue delay’. On a national basis, some Member States opt to set forth strict time limits (UK: Network and Information Systems Regulations 2018: 72 h\(^9\); Estonia: immediately, but no later than 24 h\(^{10}\)), whereas other Member States replicate the indefinite concept of ‘undue delay’ of the Directive.\(^{11}\) The amount of leeway as to the exact rules to be adopted may result in a variety of notification requirements and timeframes which do not only vary from Member State to Member State but also within sectors.

Where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident, the NCA or CSIRT may inform the public about individual incidents.\(^{12}\)

Failure to comply with the notification obligation is sanctioned via an ‘effective, proportionate and dissuasive’ administrative fine.\(^{13}\)

**The GDPR data breach notification scheme: notification obligation for data controllers**

Under the GDPR, data controllers must notify a personal data breach to the supervisory authority within 72 h after becoming aware of it, and communicate the personal data breach to the data subject without undue delay. 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’.\(^{14}\)

Notification is not required where a data breach is unlikely to result in a risk to the rights and freedoms of natural persons; for instance, where the personal data is already publicly available (Article 29 WP 2018, 18) or unintelligible to unauthorised parties (e.g. encrypted data)\(^{15}\) and a disclosure of such data does not pose a risk to the individual. The same applies to where the controller has taken steps to ensure that the high risk posed to individuals’ rights and freedoms is no longer likely to materialise.\(^{16}\) Recitals 75 and 85 enlist as potential damage *i.a.* discrimination, identity theft or fraud, financial loss, reputational damage, and loss of confidentiality of personal data protected by professional secrecy.

In contrast to the NIS Directive, the GDPR also determines the information to be forwarded, such as *i.a.* the nature of the personal data breach, including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.\(^{17}\) ‘Categories of data’ include information whether sensitive data in the sense of Art. 9(1) GDPR, or data relating to criminal convictions and offences in the sense of Art. 10 GDPR is concerned (Martini 2018).

The GDPR distinguishes between notification of the national competent authority, the Data Protection Authority and the general public. Pursuant to Art. 33(1) GDPR, the Data Protection Authority has to be informed without undue delay and, where feasible not later than 72 h after having become aware of the data breach. A controller can be considered to have become ‘aware’ of an incident when he has ‘a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised’ (Article 29 WP 2018, 11). Where notification of the DPA cannot be achieved within 72 h, information may be provided in phases without undue further delay.\(^{18}\)
Where the data breach is likely to result in a high risk to the rights and freedoms of natural persons, Art 34 GDPR requires the controller to also communicate the breach to the affected individual without undue delay. In contrast to Art. 33 GDPR, the notification obligation requires a ‘high risk’ for the rights and freedoms of the affected individual.

Other than with regard to the notification of the DPA, the notion of ‘undue delay’ is not further concretised. Undue delay is rather considered as ‘as soon as reasonably feasible’. Recital 86 further suggests that the communication to be made ‘in close cooperation with the supervisory authority respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities’.

The notice to individuals allows the controller to provide information on the risks encountered and advise individuals on how to protect themselves from the potential consequences of the breach. Controllers are free to determine the appropriate communication channel, e.g. SMS or eMail (Art. 29 WP 2018, 21). Where the direct communication to the individuals concerned would involve disproportionate effort, Art. 34(3)(c) GDPR permits a public communication or similar measure in an equally effective manner.

Mandatory communication to the data subject is not without limits. Art. 34(3) GDPR enlists three exceptions, namely where:

1. ‘the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption’;
2. ‘the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialize’;
3. ‘it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner’.

Due to their nature as exceptions to the general rule, the conditions have to be interpreted restrictively to have an effect. In particular (2) only defines the aim but does not indicate which measures may achieve said aim.

Art. 34(3) GDPR is not conclusive as Art. 23(1) GDPR, a so-called opening clause, allows further restrictions, when such restrictions respect the essence of fundamental rights and freedoms and are a necessary and proportionate measure in a democratic society to safeguard the interests enlisted in Art. 23(1) GDPR such as national or public security. Germany for instance made use of the opening clause and included further exceptions in the German federal data protection Act (‘Bundesdatenschutzgesetz – BDSG’). § 29 (1)(3) BDSG sets forth that the obligation to inform the data subject of a personal data breach shall not apply as far as meeting this obligation would disclose information which by law or by its nature must be kept secret, in particular, because of overriding legitimate interests of a third party.

Legal responsibility to notify the supervisory authority rests with controllers as does the overall responsibility for the protection of personal data. Accordingly, Art. 33(2) requires data processors solely to notify controllers of a personal data breach.
Failure to report a breach without undue delay may trigger an appropriate administrative fine of up to 10,000,000 EUR, or in the case of an undertaking, of up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Thus, controllers and processors are encouraged to put in place an incident response plan, which enables them to detect and promptly respond to a breach, as well as to assess the risk to individuals.

**Coexistence of the notification regimes**

While the NIS Directive and the GDPR notification obligations are very similar, they are not mere duplications, and do not exclude one another. It has to be noted, that the GDPR does not constitute a lex specialis to the NIS Directive in the sense of Art. 1(7) NIS Directive, which would exclude the application of the NIS Directive.

The GDPR requires breach notification only where personal data is at stake; the NIS Directive, on the other hand, mandates breach notification if there is a significant disruption to the provision of the service. While, in theory, one may distinguish between incidents falling under the GDPR and such falling under the NIS Directive, in practice, most security incidents will involve some personal data, meaning that OESs and DSPs will have to report these incidents to two different competent authorities. As DSPs typically operate as data processors, conflicts and confusion could arise between authorities, if the same incident was notified by two different entities to two different authorities, namely, the DSP under the NIS Directive and the data controller (using a service provided by the DSP) under the GDPR. Considering that format, content and timeframe are not necessarily identical, there is a likelihood that the authorities will receive information with regard to one incident, that is not identical and as a consequence, one incident will be dealt with as if there were two separate incidents.

The notification schemes also differ in so far as they require notification of the individuals concerned. If a security incident constitutes a data breach, the data controller has to notify the data subjects concerned if the data breach is likely to result in a high risk to the rights and freedoms of natural persons in order to allow him or her to take the necessary precautions. The data subject should be put in a position to prevent the risk from materialising. Other than protecting the rights and freedoms of a natural person, publicity of incidents under the NIS Directive aims at (re-)establishing information security, i.e. Confidentiality, Integrity and Availability of network and information systems. 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 (cf. Arts. 14(6) and 16(7) NIS Directive).

**The dilemma: when immediate notification of the data subject is contra the general interest of information security**

While the data subject should be in a position to take necessary precautions to prevent potential harm from materialising or limit the effects of the data breach, communication to the data subject requires the service provider to ‘go public’ about a security incident in any case. The OES or DSP cannot rely on the data subject to remain silent about an information security incident. Once users are notified, it is unlikely that these individuals will...
keep the information confidential and even if some might obey a confidentiality clause in the notification, the adversary might be among the affected users anyway. Thus, as soon as the first data subject is notified, the adversary will likely become aware that his attack has been identified.

Now any reasonable adversary will cover their tracks. However, they might not cease from further interferences at this point; it is more likely that the adversary changes its attack vector. This makes it particularly hard for the service provider, as well as law-enforcement, to identify the attacker, or to understand the vulnerabilities of a certain technology that has been used to mount the attack. Hence it is often in the interest of all honest parties to delay the notification of the data subjects. On the other hand, a less honest OES or DSP might use this argument to delay notifications for an unreasonably long period.

The following section outlines responses to security incidents highlighting the dilemma of the service provider of notification without undue delay. The different stages of the incident response cycle are presented, while pointing out the different stages at which notifications might be due. Notably, these points in time are easy to identify in a post hoc analysis, but hard to recognise during an active attack.

**Incident response cycle**

Among the organisational measures for information security, a structured, methodical handling of computer incidents is crucial. Incident response needs to follow a clear cycle to quickly contain, minimise, and ultimately learn from the incident. The incident response cycle of the U.S. National Institute of Standards and Technology (NIST)\(^\text{24}\) has become one of the two industry standards in this field. It provides guidance in form of an incident response cycle with four phases, where each phase feeds its results into the next, and the last phase feeds its lessons learned into the first again: (1) Preparation, (2) Detection and Analysis, (3) Containment and Recovery, and (4) Post-Incident Activity (Cichonski et al. 2012).

During the Preparation phase (Cichonski et al. 2012, 21–24) general organisational measures are taken, in particular responsibilities and lines of report and command are established, most notably system owners for each subsystem are identified. This structure is then used for a risk assessment; hence assets and their owners are identified, valued and the probability of loss are evaluated. For the latter, attack vectors need to be identified and appreciated if they can be a threat. Finally, prevention and protection measurements are put in place answering the potential threats, that help to either reduce the value of an asset or lower the probability of loss.

The Detection and Analysis phase (Cichonski et al. 2012, 25–34) is hopefully the state of normal operation. System owners have to continuously monitor identified attack vectors, signals, and indicators to assess the current state of the IT system. Detected anomalies are assessed, documented and trigger notifications are issued to the incident response team of the OES or DSP, which in turn will run its assessment and inform other system owners.

Once an attack is detected, the Containment and Recovery phase (Cichonski et al. 2012, 35–38) starts. The first goal is to identify effected systems, and to avoid further spread and damage caused by the attack. Next, evidence is collected about the mechanisms and effects of the attack which is used to repair systems, and to attribute the attack to an
adversary. The latter might help to take legal steps against them, but also helps to taketechnical protection measures against attacks from the same source.

In the last, the Post-Incident Activity, phase of the cycle (Cichonski et al. 2012, 38–42),evidence is archived, and recommendations are compiled. These recommendations willbe used as feedback to improve the preparedness for future attacks, so the responsecycle starts anew.

As regards linearity and concurrence, the following must be noted: There might beback tracking within one run of the cycle, if new evidence makes this necessary. Inaddition, attacks might run in parallel resulting in parallel running responses. And ofcourse, two initially independently started responses might turn out to be caused bythe same attack.

**Mapping of scenario: when does the clock start to tick?**

Besides a technical response to the attack, legal response needs to be prepared. Thisincludes steps to ensure legal compliance with the applicable norms. For the purposeof this article, the primary question is whether end users need to be notified, and if so when.

For the GDPR, an end user, i.e. the data subject, needs to be notified if according to Art.34(1) GDPR, the leaked data ‘is likely to result in a high risk to the rights and freedoms ofnatural persons’, and none of the exceptions to refrain from data subject/general publicnotification applies, i.e. data was not unintelligible or the controller has not taken subse-quent action to mitigate the risk for rights and freedom of data subject. Now knowledgeof an attack requires notification without ‘undue delay’, i.e. according to Recital 86, GDPR‘as soon as reasonably feasible’.

However, this requires the data controller to determine which phase in the responsecycle triggers a ‘reasonable’ obligation to inform under Art. 34 GDPR. Besides under-standable business reasons, such as reputational loss, risk of liability claims by users, to delay or even refrain from data subject notification, there are also comprehensible technicalreasons to delay going public with information about a security breach.

**Time line of an attack.** An attack starts with a potential attacker probing a system to understand exploitable vulnerabilities, and then choosing tools and making preparationsin its own systems. If the attacker then successfully mounts an attack, a security breachhappens. This might lead to the leakage of data, or to disturbance, or interruption ofthe attacked service. Depending on the attackers aims, it might continue to run theattack until stopped, or it might decide that it has achieved its goal (or that the attackis becoming too risky for itself) and stops. In the latter case, it might take action to remove evidence from the system.

These attack phases match roughly with the following phases of the response cycle:Information that can be learned by potential probing should be analysed during prep-aration with regard to its attack potential. Moreover, probes might be detectable andshould be detected during detection. Since the mere probing does not establish a securitybreach, notifications to supervisors are debatably at most: if large scale probing is observed, it might help to prevent attacks on other similar systems. However, while this might be very desirable, there is little to no evidence to the outside if a systemwas probed and an attack was successful prevented.
Given the attack is actually successful mounted, it should be detected during phase 2. However, a single attack most certainly will trigger several indicators. So, analysis in phase 3 is needed. This in turn might lead to the discovery of further indicators, which makes back tracking necessary. This leaves the question, how long the back and forth between 2 and 3 would be acceptable until the response team has to move to phase 4. Post-Incident Activity within phase 4 certainly at some point triggers the legal notification obligations if the attack reaches the critical threshold.

**No undue delay: prevailing and legitimate interest in suspending data subject notification**

The time line of an attack and the NIST response cycle highlights that a OES or DSP may have a comprehensible interest to delay the notification of individuals as required under Art. 34 GDPR, and hence go public about an incident. The research mode within phase 2 requires the OES or DSP to gather as much information as possible on the incident and analyse it. Determination of the entry point and the breadth of the breach is necessary. Early release of information in the response cycle may not only interfere with subsequent containment and recovery, it may also hinder identification of the attacker or prevent monitoring of his techniques and communication means. Delaying communication of a personal data breach to the individual, however, interferes with the obligation to inform ‘without undue delay’. As outlined above, in the context of Art. 34 GDPR, recital 86 refers to undue delay as ‘as soon as reasonably feasible’. What can be considered as reasonable feasible is hardly addressed in the GDPR or the NIS Directive insofar as the interplay of these instruments is concerned.

The NIS Directive recognises the necessity to suspend notification of the public under the NIS Directive in Recital 59, which requires that publicity of incidents should duly balance the interest of the public in being informed about threats against possible reputational and commercial damage for OESs and DSPs reporting incidents. Publicly sharing information about a vulnerability may also reveal too much of the entities’ NIS infrastructure and operation (cf. Weulen Kranenbarg, Holt, and van der Ham 2018). This brings a further aspect into play, namely core business interests of the service providers, that deserve equal protection as the interest of the public to be informed about security incidents. Recital 59 further states that ‘in the implementation of the notification obligations, competent authorities and the CSIRTs should pay particular attention to the need to keep information about product vulnerabilities strictly confidential, prior to the release of appropriate security fixtures’. This, however, requires that the response cycle outlined above has been fully completed, meaning that incident publicity can be delayed until technical protection measures addressing the vulnerability are in place.

Following this conclusion, the NIS Directive is obviously conflicting with Art. 34 GDPR, where the risk to the rights and freedoms of a natural persona would call for prompt communication with data subjects to mitigate potential adverse effects. Recital 86 GDPR recognises the need to respond to an attack as a justification to delay such prompt communication: ‘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’. This justification is however limited to continuing and ongoing data breaches and
does not encompass ongoing security incidents as such. Hence it would 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.

Although the legislator recognised a reasonable interest to suspend notification as such, there is no explicit exception from the ‘without undue delay’ notification obligation of data subjects in Art. 34 GDPR.

Considering that the data controller needs to analyse the attack in order to device an appropriate containment strategy, delaying the publicity of incidents has been referred to as ‘responsible disclosure’ (Laue 2019, marginal no. 10 with further references). ‘Responsible disclosure’ obviously fell off the radar of the legislator, as the recitals limit their focus on the interests of law enforcement when the suspension of notification is addressed. Accordingly, recital 88 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’. Hence, a delay can be justified in the interests of law-enforcement authorities, i.e. the execution of criminal investigations. This requires that law enforcement authorities are involved in the incident response conducted by the service provider. In that regard, Art. 8(6) and Recital 62 NIS Directive encourages the consultation and cooperation of competent authorities, single point of contacts and respectively the providers concerned with the relevant national law enforcement authorities and national DPAs. Member States should further encourage OESs and DSPs ‘to report incidents of a suspected serious criminal nature to the relevant law enforcement authorities’.25 Therefore, severe incidents are very likely to be reported to national law enforcement authorities – either by the provider or a supervisory authority. Considering that a prerequisite for the notification obligation under NIS Directive is a certain degree of severity of the incident and illegal access and illegal interception of non-public transmissions of computer data as well as data and system interferences constitute crimes under the Convention on Cybercrime of the Council of Europe,26 reportable incidents are likely to result in criminal investigations if a malicious attack is assumed. However, at the beginning of an incident, it is often not clear if an actual attack is ongoing, or if the incident was caused by human error or events, that are not computer security-related, such as natural disasters, power failures, or failing material (Cichonski et al. 2012, 6). This means that it is difficult to determine ex ante and in abstracto when and if law enforcement will be involved.

In the case of law enforcement being involved and a criminal investigation, personal data will also be processed by law-enforcement authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences, resulting in the application of the Police Directive.27 The Police Directive allows for national legislative measures delaying, restricting or omitting the provision of information to the data subject to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to inter alia avoid obstructing official or legal inquiries or investigations.28 It would contravene the ratio of said norm and hamper investigations, if a data controller was obliged to inform the public of an incident.
However, where an incident does not trigger the involvement of law-enforcement authorities, the data controller is still faced with the legitimacy of suspending notification. While for the NCA under the NIS Directive the aforementioned ‘responsible disclosure’ will obviously constitute a necessity for appropriate incident handling, the DPA, primarily concerned with the rights of the data subject, may not share this technical viewpoint. As regards the relationship of the competent authorities under the GDPR and the NIS Directive, Art. 15(4) NIS Directive establishes that the competent authority under the NIS Directive shall work in close cooperation with DPAs when addressing incidents resulting in personal data breaches.

Recital 63 specifies that in the context of compromised personal data, said authorities ‘should cooperate and exchange information on all relevant matters to tackle any personal data breaches resulting from incidents’. This recital highlights the need to mitigate the impact of personal data breaches, while recognising that such mitigation requires the cooperation of national authorities which have different expertise. Expertise in the field of information security does not necessarily mean that the NCA under NIS Directive may pay the necessary regard to the mitigation of personal data breaches. Likewise, DPAs may lack the understanding of the different stages of an incident response cycle. Hence, ‘responsible disclosure’ can only be put in practice if the competent authorities cooperate and provide coherent advice to the data controller concerned: a lack of cooperation between the authorities would result in the data controller being left in limbo.

The dilemma may even be more complicated, where an OES relies on a service provided by a DSP, for instance, cloud computing: in this scenario, the OES would be obliged to notify a security incident to the DPA as he remains the data controller, whereas the DSP would have to notify the competent NIS authority. As a result, one incident would be reported under two different regimes by two different actors under different timeframes and very likely with non-identical yet similar information. It cannot be ruled out that the DPA may not be aware that the incident notified by the DSP to the NCA, and the data breach independently notified by the OES relate to the same attack, and thus one single incident may be treated differently. Considering that the OES will most likely not be actively involved in the response cycle of the DSP, the OES is dependent on the content of status updates provided by the DSP to determine the time for disclosure to the data subject. If mandatory or voluntary cooperation mechanisms between the concerned authorities were missing, there would be an even greater risk of early disclosure.

Conclusions and recommendations

In light of the foregoing, Member States are advised to make close cooperation of NCAs with DPAs when addressing incidents resulting in personal data breaches mandatory. The amount of leeway given to Member States (‘shall work in close cooperation’29) disregards the risks attached to early incident disclosure.

In a broader context, it has to be noted that the dilemma of co-existing similar incident notifications obligations is not limited to the NIS Directive and the GDPR. The legislator identified in Art. 1(3) NIS Directive pre-existing sector-specific EU legal regimes, i.e. Directive 2002/21/EC30 and Regulation (EU) No 910/2014 (eIDAS Regulation),31 that had already introduced security measures and notification obligations regarding security incidents.
Similar notification obligations also exist under further EU legal instruments such as the Second Payment Services Directive (PSD2). Consequently, operators of IT infrastructure may be faced with diverse reporting obligations to different competent authorities depending on the service under attack. The multitude of obligations may even arise within one single sector due to for instance different supervisory levels, as well as national and EU levels. In particular, entities that engage in cross-border activities face different regulatory requirements, that may overlap (European Commission 2020).

An example of such fragmentation of incident reporting obligations is the financial sector (EBF 2020): Financial institutions operating in the EU face a variety of incident reporting obligations, i.e. under GDPR (as a ‘personal data controller or processor’), PSD2 (as a ‘payment service provider’), NIS Directive (as an ‘OES’), ECB/SSM (as a ‘significant institution’), eIDAS Regulation (as a ‘trust service provider’) and ECB/Target2 (as a ‘Target2 critical participant’). Varying reporting timeframes from 2 h (ECB) to 72 h (GDPR) to non-concrete timeframes (NIS Directive) combined with different addressees, and information to be forwarded may result in a scenario where different authorities may receive non-identical information at different times.

Where notification schemes are decentralised and non-homogenous as in the example above, overlaps are likely. Considering that information exchange as well as a coordinated course of action between the competent authorities/bodies may not be prescribed by national law, decentralisation complicates matters even further.

An instrument for coherence could be the introduction of a mandatory joint reporting scheme with a central hub for notifications – meaning that the centralised approach employed by a slight majority of Member States under the NIS Directive is taken one step further. A single national competent reporting body has more control over the information notified by OESs and DSPs, and thus, a clearer view on all incidents. A single competent authority also facilitates cross-border consultation. The joint reporting body could then not only advise the notifying entity on public disclosure, but most importantly, the information exchange and thus preparedness against vulnerabilities at a larger scale could be safeguarded.

As regards Confidentiality, Integrity and Availability, knowledge about vulnerabilities is key. As of now, it is up to the national legislators to introduce cooperation mechanisms between the different authorities/bodies involved. These mechanisms require a certain level of liaison competence in all relevant authorities. The NIS Cooperation Group acknowledged that in order to benefit from synergies, a national policy taking into account all constraints and opportunities is needed (2018).

Finally, it must be recalled, that the NIS Directive as such recognises communication and cooperation as a key element for an increased level of cyber resilience. In that sense, national single points of contact are responsible for coordinating issues related to the cross-border cooperation of Member State authorities and with the relevant authorities in other Member States. However, cooperation must not only be mandatory in case of cross-border cooperation, it needs to start at national level with clear rules on information exchange, coordination and cooperation, among various national competent bodies. Bearing in mind that the core idea of incident reporting is to gain insight, understand challenges, offer assistance to the entities concerned, and thereby increase the overall level of resilience, notifications are merely the first step that allows to detect similarities, common threats and targets of incidents. Naturally, collected data needs to be
analysed across sectors on the national level as well as across Member States. Failing either cooperation level leaves incident notification to be a blunt sword against attacks.

Notes

1. 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), OJ L 119, 04.05.2016, pp. 1–88.
2. 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, OJ L 194, 19.07.2016, pp. 1–30.
3. OES must be identified as such on a national basis by Member States.
4. Providers of digital services have to self-determine whether they offer services of a type listed in Annex III of the NIS Directive[4] in order to fall within the scope of application of the Directive.
5. Art. 5(2) NIS Directive enlists as criteria inter alia whether the entity provides a service which 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. These criteria resemble 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, OJ L 345, 23.12.2008, pp. 75–82) with the difference that only entities depending on NIS may qualify as OESs, and thus fall within the scope of the NIS Directive.
6. The NIS Directive provides for great flexibility either to implement a centralised or decentralised approach for designation of 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 depends on whether the operator concerned is an OES or DSP (Cf. Art. 9(1) Real Decreto-ley 12/2018 de 7 de septiembre de seguridad de las redes y sistemas de información); the same applies to the UK, where the NCA for OES further depends on the sector concerned.
7. According to Art. 9 NIS Directive, Member States shall designate one or more CSIRTs, which may be established within a NCA and must be responsible for risk and incident handling.
8. See Art. 14(3) NIS Directive as regards OES, and Art. 16(3) as regards DSP. Guidelines for incident reporting by DSPs have been issued by ENISA, see ENISA 2017.
9. Sec. 11(3)(b)(i) UK Network and Information Systems Regulations 2018 for OES and sec. 12 (6)(a) UK Network and Information Systems Regulations 2018 for DSPs.
10. This applies only to OES, see § 8(1) Küberturvalisuse seadus.
11. For instance Germany, see § 8b(4) BSIG.
12. Arts. 14(6) and 16(6) NIS Directive.
13. What is considered “effective, proportionate and dissuasive” varies significantly between Member States, with administrative fines of up to EUR 50,000 in Germany (§ 14(2) BSIG) and fines of up to GBP 17,000,000 in the UK (Art. 18(6)(d) Network and Information Systems Regulations 2018).
14. Art. 4(12) GDPR.
15. Art. 34(3)(a) GDPR.
16. Art. 34(3)(b) GDPR.
17. See Art. 33(3) GDPR.
18. Art. 33(4) GDPR.
19. Art. 34 GDPR; see also Recital 86.
20. Recital 86.
21. Recital 86.
22. This exception distinguishes between two types of information: information which by law must be kept secret and information which by its nature must be kept secret. Information which by law must be kept secret relates to professional obligations to secrecy which build on a special position and usually relate to psychologists, notaries or lawyers as long as their professional associations have issued binding rules on secrecy. Special official obligations to maintain secrecy relate to obligations that are linked to the exercise of a public office. In assessing whether an information must be kept secret by its nature, due consideration has to be paid to the purpose of the data as such and the purpose of the data processing operation; the obligation to “secrecy” must stem directly from the type of the information (Uwer 2020, marginal no. 8). Also, there may be an interest to keep the source of information secret. This exception further requires a balancing of interest of the data subject concerned on being informed about the data breach and the interest to keep the information secret.

If the interests of the data subject, in particular in consideration of impending damage, outweigh the interest in secrecy, the data subject shall be informed.

23. Art. 83(4)(a) GDPR. See also (Art. 29 WP 2017).
24. NIST is a U.S. government agency and part of the U.S. Department of Commerce.
25. Recital 62 NIS Directive.
26. Council of Europe, Convention on Cybercrime (CETS No. 185).
27. Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Police Directive), (2016) OJ L 119, 04.05.2016, pp. 89–131.
28. See Art. 13(3) Police Directive.
29. Art. 15(4) NIS Directive.
30. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJL 108/33, 24.4.2002. Now replaced by Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ L 321, 17.12.2018, pp. 36–214.
31. 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, OF L 257, 28.08.2014, pp. 73–114.
32. 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, OJ L 337, 23.12.2015, pp. 35–127.
33. Art. 96(1) 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, OJ L 337, 23.12.2015, pp. 35–127 (PSD2) requires payment service providers, without undue delay, to notify the competent authority in the home Member State in the case of a major operational or security incident.
34. The ECB Banking Supervision has implemented a cyber-incident reporting framework within the Single Supervisory Mechanism.
35. TARGET2 = Trans-European Automated Real-Time Gross Settlement Express Transfer System is the real-time gross settlement system for the Eurozone.
36. By decentralised, we refer to a multitude of supervisory authorities under sector-specific regulation due to a lex specialis to the NIS Directive or because the Member State opted for a decentralised approach to designate NCAs and single points of contact. 13 Member States (previously 14 including the UK) decided to designate several sectoral authorities.
37. Cf.FN 6.
38. See Art. 8(4) NIS Directive and Recital 31.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

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/.

References

Art. 29 Data Protection Working Party. 2017. “Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation 2016/679”. WP 253.

Art. 29 Data Protection Working Party. 2018. “Guidelines on Personal Data Breach Notification Under Regulation 2016/679”. WP250 rev.01.

Cichonski, P., T. Millar, T. Grance, and K. Scarfone. 2012. “NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide Recommendations”. NIST Special Publication. doi:10.6028/NIST.SP.800-61r2.

ENISA. 2017. “Incident Notification for DSPs in the context of the NIS Directive”. https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive/at_download/fullReport.

European Banking Federation. 2020. “EBF Position on Cyber Incident Reporting”. https://www.ebf.eu/wp-content/uploads/2020/06/EBF-position-paper-on-cyber-incident-reporting_annex-on-FLIIS.pdf.

European Commission. 2020. “Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity Across the Union, Repealing Directive (EU) 2016/1148”. COM(2020) 823 Final.

Halevi, T., N. Memon, and O. Nov. 2015. “Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-efficacy and Vulnerability to Spear-Phishing Attacks”. doi:10.2139/ssrn.2544742.

Hansen, M., M. Jensen, and M. Rost. 2015. “Protection Goals for Privacy Engineering”. IEEE Security and Privacy Workshops. https://ieeexplore.ieee.org/document/7163220.

Laue, P. 2019. “Art. 34 DSGVO.” In Recht der elektronischen Medien, edited by G. Spindler and F. Schuster. München: C.H. Beck.

Martini, M. 2018. “Art. 33 DSGVO.” In Beck’sche Kompakt-Kommentare, Datenschutz-Grundverordnung Bundesdatenschutzgesetz, edited by B. Paal and D. Pauly. München: C.H. Beck.

NIS Cooperation Group. 2018. “Reference Document on Incident Notification for Operators of Essential Services”. CG Publication 02/2018. https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_incident_reporting_00A3C6D5-9BDB-23AA-240AF504DA77F0A6_53644.pdf.

Uwer, D. 2020. “§ 29 BDSG.” In Beck’scher Online-Kommentar Datenschutzrecht, edited by S. Brink and H. A. Wolff. München: C.H. Beck.

Weulen Kranenbarg, M., T. J. Holt, and J. van der Ham. 2018. “Don’t Shoot the Messenger! A Criminological and Computer Science Perspective on Coordinated Vulnerability Disclosure”. 7 Crime Science 16. doi:10.1186/s40163-018-0090-8.