Don't Put the Cart Before the Horse – Effective Incident Handling Under GDPR and NIS Directive

Sandra Schmitz-Berndt, Stefan Schiffner

Note: The title of this paper was changed after the manuscript was submitted for publication. The revised title of the paper is:

> Don’t Put the Cart Before the Horse – Effective Event Handling Under GDPR and NIS Directive

Don't Tell Them now (or at all) – End User Notification Duties under GDPR and NIS Directive*

Sandra Schmitz-Berndt[1] and Stefan Schiffner[2]

[1] Université du Luxembourg, Esch sur Alzette, Luxembourg
Sandra.Schmitz@uni.lu
[2] Université du Luxembourg, Esch sur Alzette, Luxembourg
Stefan.Schiffner@uni.lu

Abstract. This paper serves as notes to a lecture given at the IFIP summer school of privacy and identity management 2020. We discussed notification requirements in the NIS directive and the GDPR in the case of security and privacy incidents form legal and technical perspective. In particular, we discuss timing. While a need to mitigate an immediate risk of damage for an individual would call for prompt communication with data subjects, there are scenarios which may justify a delay in communication to a wider public, e.g. a large user base. This might be advisable, for instance, where a service provider needs to analyse the current attack to prevent further attacks and assess the full impact. In the latter, any delay in communication should fulfil the requirement of "without undue delay". Further, we discuss why the concurrent reporting under both regimes is needed and conclude with a call for more cooperation of the respective competent authorities.

1 Introduction

This paper contains work in progress and reflects a snap shoot of our research taken at the time of the lecture. The final results of our work are under publication and will appear later this year [1].

The field of cybersecurity in 2016 saw two important legal instruments adopted: the omnipresent General Data Protection Regulation[3], and the underappreciated Network and Information Systems Directive[4]. The objective of both instruments

* Both authors are supported by the Luxembourg National Research Fund as part of EnCaViBS project, grant number C18/IS/12639666/EnCaViBS/Cole.

[3] 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.

[4] 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

is to ensure appropriate security of information technology (IT) systems and the data processed by those.

While both instruments are largely in alignment, particularly with their risk-based approach to security measures, they have distinct interests: the GDPR covers privacy rights concerning personal data of individuals, while the NIS Directive encompasses the information security, i.e. the confidentiality, integrity and availability (CIA), of the services covered and the underlying information technology infrastructure. In many cases, the latter does include personal data, meaning that the NIS Directive can be regarded as a complementary law to the GDPR. 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 as regards addressees, which only include operators of essential services (OES) and digital service providers (DSP).

Both instruments introduce similar notification obligations based on the assumption that security threats can only be eliminated if security risks and data breaches are communicated to public authorities. The NIS Directive requires OES' and DSPs to notify, without undue delay, the competent national authorities of security incidents having a significant impact on the continuity of the services they provide. Where an incident simultaneously constitutes, or becomes, a personal data breach, the provider needs to inform the data protection regulator separately under the GDPR without undue delay and within 72 hours. In practice, two separate regulators may have to be informed about the same incident.

In addition, under Art. 34 (1) GDPR, the provider shall communicate a personal data breach without undue delay to the data subject if the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. However, Art. 34 (3) GDPR foresees exceptions to the notification obligations and enlists conditions under which the communication to the data subject shall not be required. Member States may provide for further derogations to Art. 34 (1) GDPR, of which some will be outlined.

The reminder of this paper is organized as flows: First we map the notification obligations and the roles of the regulators. Second from an interdisciplinary perspective, we will present dilemma scenarios in which none of the exceptions for immediate notification applies, but nevertheless the provider has a prevailing and legitimate interest in suspending end user notifications. Taking the incidence response cycle as guide, we discuss, when the "clock starts to tick" for notification without undue delay.

2 Background

2.1 Information Security vs Privacy

Information security and privacy interact in a complex fashion: A breach in one might lead to an incident in the other field. While it might be obvious that unauthorized access to a data base (IT-Security incident) containing, e.g., VISA card

information, is a privacy breach, the other way around might be less obvious. However, personal information leaked, might be used in spearfishing attack, e.g., the attacker might learn that a targeted person is client of a specific bank, given this information a more convincing spearfishing email can be tailored changing significantly the chances that the victim is tricked into revealing sensitive information such as logins or passphrases.

So, this backdrop set: 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 takers. Traditionally in information security, we distinguish three dimensions: CIA, i.e. Confidentiality, Integrity, and Availability. Note, any practical system requires always 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 taker, the main protection goal is availability and the main adversary is an external attack that attempts to modify messages.

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 to use 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 takers here. The main protection goal is thus confidentiality to prevent an external attack from the abuse of personal data, e.g. in an identity theft scheme.

Hence, CIA is relevant for information security and personal data protection, though with some differences in emphasize of the dimensions. For privacy, the literature further distinguishes 3 more protection goals: unlikability, transparency and intervenability [2]. Here unlikability means that 2 artifacts concerning the same context, cannot be related to this context by an unauthorized party. Hence this could be seen as confidentiality of meta data; 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 norms, GDPR and NIS Directive, reflect these protection goals; w.r.t. the notification obligations. For the first these obligations concern mainly confidentiality and unlikability breaches, while for the latter the main concern is disruptions of service, hence availability breaches.

2.2 Incident Handling under NIS Directive and GDPR

A key element of data security is prevention and if nevertheless a data breach occurs, to be able to react in a timely manner. If a breach of personal data or

a security incident occurs, the GDPR and the NIS Directive both introduce the requirement for said incident to be notified to the competent national authority. Similar notification obligations of security incidents exist under other EU legal instruments, such as Art. 19(2) Regulation (EU) 910/2014 (eIDAS Regulation)[5], Art. 96 Directive 2015/2366/EU (PSD2)[6] and Art. 40(2) Directive (EU) 2018/1972 (EECC)[7]. As regards personal data breaches Art. 4 Directive 2002/58/EC (ePrivacy Directive) contains a notification obligation limited to providers of publicly available electronic communications services.[8] The following sections outline the notification procedures under NIS Directive and GDPR.

The NIS Directive Incident Notification Scheme: Notification Obligation for OESs and DSPs. The NIS Directive is the first instrument to introduce an IT security incident notification regime across different sectors at European level. The notion of "incident" is defined in Art. 4 NIS Directive as "any event having an actual adverse effect on the security of network and information systems" with network and information systems being "interconnected systems that process, transmit and store data".

As regards the obligation to report an incident, the NIS Directive differentiates between operators of essential services (OESs) and digital service providers (DSPs). Art. 4(4) NIS Directive defines an OES as a public or private entity within one of the sectors enlisted in Annex II, which meets the criteria laid down in Article 5(2). These criteria resemble the definition of "critical infrastructure" in Art. 2(1) ECI Directive[9] with the difference that only entities depending on network and information systems may qualify as OESs and thus fall within the scope of the NIS Directive. Member States are supposed to define essential services and identify OES mwithin their territories. In contrast, Annex III of the NIS Directive enlists as DSPs to which the NIS Directive applies only three types of services: cloud services, online market places and search engines.

According to Art. 14(3) and Art. 16(3) NIS Directive, Member States shall ensure that OESs and DSPs notify, without undue delay, the competent author-

[5] Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market.

[6] 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.

[7] 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.

[8] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.07.2002, pp. 37-47.

[9] 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.

ity 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 encompassed (in case of a DSP).

The NIS Directive provides limited guidance as to what constitutes a "significant" or "substantial" impact. As regards OES, the sample parameter listed in Art. 14(4) NIS Directive to determine the significance of an impact, are of a very general nature. They for instance include the number of users affected by the disruption of the essential service, the duration of the incident, or the geographical spread without setting any thresholds. The amount of leeway as to the exact rules to be adopted in Member States may result in various notification requirements which do not only vary from Member State to Member State, but also from sector to sector. Thus, a Member State may also refrain from setting any specific requirements, leaving the service concerned to determine whether an incident had a substantial or significant impact. Considering the legal nature of a Directive, Member States are also free to impose stricter reporting requirements than those laid down in the Directive. As a result, Germany for instance obliges OESs to also notify larger "near misses".[10] Guidance at EU level is provided for the determination of "substantial impact" with regard to DSPs by the Commission Implementing Regulation (EU) 2018/151[11]. The Implementing Regulation accepts that an incident has a substantial impact where for instance the service provided by a digital service provider was unavailable for more than 5,000,000 user-hours whereby the term user-hour refers to the number of affected users in the Union for a duration of 60 minutes, or the incident has resulted in a loss of integrity, authenticity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via a network and information system of the digital service provider affecting more than 100,000 users in the Union.[12] Failure to comply with the notification obligation is sanctioned via an "effective, proportionate and dissuasive" administrative fine.[13] Of relevance for this paper is the timeframe within which an incident must be reported and the addressee of said notification. Although from the Directive as such, the ad-

[10] § 8(4)(2) BSIG.

[11] 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, OJ L26, 31.01.208, pp.48-51.

[12] Further where (c) the incident has created a risk to public safety, public security or of loss of life; (d) the incident has caused material damage to at least one user in the Union where the damage caused to that user exceeds EUR 1,000,000, see Art. 4 Implementing Regulation (EU) 2018/151.

[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).

dressee seems clear, it has to be noted, that a variety of competent authorities exist. This is due to the fact, that almost half of all Member States opted for a decentralised approach in regulation, meaning that potentially each sector has its own competent authority. In practice, there is a fragmentation of competent authorities across the EU. As regards the timeframe, the NIS Directive only refers to the indefinite concept of "without undue delay". Again, considering the amount of leeway given to Member States, a fragmentation of reporting timelines exists with a tendency to replicate the indefinite concept of "undue delay" of the Directive. Ultimately, Art. 14(6) and 16(6) NIS Directive further foresee (after consulting the notifying entity), that the competent authority or 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.

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 (DPA) within 72 hours 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 in Art. 4(12) 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". The test whether a breach occurred and has to be reported is a mere objective test [3], marginal no. 16a. The main difference to the NIS Directive is, that the GDPR only applies to security incidents that concern personal data.

The WP 29 categorises data breaches according to the following information security principles: (1) confidentiality breach, where there is an unauthorised or accidental disclosure of, or access to, personal data; (2) integrity breach, where there is an unauthorised or accidental alteration of personal data; (3) availability breach, where there is an accidental or unauthorised loss of access to, or destruction of, personal data [4].

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 [4] or unintelligible to unauthorised parties (e.g. encrypted data)[14] and a disclosure of such data does not pose a risk to the individual. 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.[15] Potential damage may be discrimination, identity theft or fraud, financial loss, reputational damage, and loss of confidentiality of personal data protected by professional secrecy. According to Art. 33(3) GDPR requires the controller to provide detailed information to the DPA including measures to mitigate possible adverse effects of the breach. Legal responsibility to notify the DPA rests with controllers as does the overall responsibility for the protection of personal data. Accordingly, Art. 33(2) requires data processors solely to notify

[14] Art. 34(3)(a) GDPR.
[15] Art. 34(3)(b) GDPR.

controllers of a personal data breach. Relevant for this paper is the timeframe, within which the controller has to notify the DPA of a data breach. Unlike the NIS Directive, the GDPS concretices the notion "without undue delay" by specifying that, where feasible, notification is required not later than 72 hours after having come beware 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" [4]. Recital 85 clarifies that where notification of the DPA cannot be achieved within 72 hours, information may be provided in phases without undue further delay. In this case, the reasons for the delay must be communicated to the DPA. In addition to the required notification of the DPA, Art. 34 GDPR also requires the controller to communicate the breach to the affected individual without undue delay, where the data breach is likely to result in a high risk to the rights and freedoms of natural persons. 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".[16] Art. 34(3) GDPR lists derogations from the mandatory communication to the data subject. These include protection measures by the controller, that render the personal data unintelligible to any person who is not authorised to access it, such as encryption. The exceptions are rather vague and the conditions for exemption from a notification obligation are indefinite. It has to be noted that 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 this 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 according to Art. 34 GDPR 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.[17] Failure to report a

[16] Recital 86.

[17] The 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 [5], 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.

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.[18]

Coexistence of the Notification Regimes. While the NIS Directive and the GDPR introduce notification regimes that are in practice very similar, the obligations are not identical and do not exclude one another. 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, requires incident 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 can potentially be treated as 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 gain knowledge 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).

3 The Dilemma: When Immediate Notification of the Data Subject Contradicts 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

[18] Art. 83(4)(a) GDPR. See also [6].

breach, communication to the data subject means in any case, that the service provider has to "go public" about a security incident. In practice, it is unlikely that data subjects 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 notification is out to a data subject, the adversary is likely to become aware that his attack has been identified.

Now any reasonable adversary will start covering its 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 harder 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 data subject notification. On the other hand, a less honest OES or DSP might use this argument to delay notifications unreasonable long.

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 recognize during an active attack.

Incident Response Cycle. Among the organizational measures for information security, a structured handling of computer incidents is crucial. NIST is providing guidance introducing an incidence response cycle with four phases, each feeding its results into the next and the last phase is feeding its lessons learned into the first again: (1) Preparation, (2) Detection and Analysis, (3) Containment and Recovery, and (4) Lessons learned [7].

During Preparation general organizational 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.

Detection and Analysis. This phase is hopefully the state of normal operation. System owners are the continuously monitoring the before identified attack vectors, signals, and indicators to assess the current state of the IT system. Detected anomalities are assessed, documented and trigger notifications to the incident response team of the OES or DSP, which in turn will run its assessment and inform other system owners.

Containment and Recovery. After an attack was detected its analysis needs to result in a containment strategy. 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 this 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 take technical protection measures against attacks from the same source.

Lessons Learned. In the last phase of the cycle, evidence is archived and recommendations are compiled. These recommendations will be used as feedback to improve the preparedness for future attacks, so the response cycle starts anew.

Two notes: There might be back tracking within one run of the cycle if new evidence is making this necessary. Moreover, Attacks might run in parallel which leads to parallel running responses. Corollary, 2 initially independently started responses might turn out to be caused by the same attack.

Mapping of the scenario: When does the Countdown start? Besides a technical response to the attack, legal responses need to be prepared. This includes steps to ensure legal compliance with the respective norms. To the end that this concerns the paper at hand, the question is if end users need to be notified or not, and if so when.

For the GDPR, data subjects need to be notified if the leaked data "is likely to result in a high risk to the rights and freedoms of natural persons"[19] and none of exceptions to refrain from data subject/general public notification applies, i.e. data was not unintelligible or the controller has not taken subsequent action to mitigate the risk for rights and freedom of data subject. Awareness of an attack requires notification without "undue delay", i.e. according to Recital 86, GDPR "as soon as reasonably feasible".

However, this leaves the data controller with the question which phase in the response cycle triggers a "reasonable" obligation to inform under Art. 34 GDPR. Beside the obvious desire to delay or even avoid to inform users about a breach, such as reputational loss, risk of liability claims by users, there are good technical reasons to delay to go public with information about a security breach.

Time Line of an Attack. An attack starts with probing a system to understand exploitable vulnerabilities. Second, the attacker choses its tools and takes preparations in its owns systems. Now the attacker can actually mount the attack and if successful, a security breach happens. This might lead to the leakage of data or to disturbance or interruption of the attacked service. Depending on the attackers aims, it might continue to run the attack until stopped or it might assess that it reached its goal (or the attack gets too dangerous for itself) and stop. 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 preparation w.r.t. to its attack potential. Moreover, probes might be detectable and should be detected during detection. Since the mere probing

[19] Art 34(1) GDPR.

does not establish a security breach, 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 system was 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. So the open question is: how long would the back and forth between 2 and 3 be acceptable until the response team moves to phase 4 which certainly needs to include informing users and authorities if the attack fulfils the conditions for notification requirements.

No Undue Delay: Prevailing and Legitimate Interest in Suspending Data Subject Notification. The scenario highlighted that a service provider may have a legitimate interest to delay the notification of individuals as required under Art. 34 GDPR, and hence go public about an incident. Any delay in communication, however, interferes with the obligation to inform "without undue delay", i.e. to inform "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 addresses the necessity to suspend notification of the public 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. 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, an explicit exception is lacking.

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" [8], marginal no. 10 with further references). "Responsible disclosure" has been ignored by the legislator, as the recitals only consider suspension of notification in the interests of law-enforcement. 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, it is accepted that 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 encourage OESs and DSPs "to report incidents of a suspected serious criminal nature to the relevant law-enforcement authorities".[20] Hence, severe incidents are very likely to be reported to national law-enforcement authorities – either by the provider or a supervisory authority. 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,[21] However, in 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 natural causes (disaster, failing material). In the case of 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[22], which explicitly 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

[20] Recital 62 NIS Directive.

[21] Council of Europe, Convention on Cybercrime (CETS No. 185).

[22] 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.

obstructing official or legal inquiries or investigations.[23] 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 still has to determine, whether suspending notification can be legitimate. While for the competent authority under the NIS Directive the aforementioned "responsible disclosure" is a necessity of an appropriate response cycle, the DPA, prioritising the rights of the data subject, may not share this technical viewpoint. A uniform approach would require cooperation of the authorities; otherwise contravening decisions are likely. As regards cooperation of the competent authorities, Art. 15(4) NIS Directive foresees that the competent NIS authority 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 recognizing 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 national NIS authority may pay the necessary regard to the mitigation of personal data breaches. Vice versa, national 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 communicate and advise the data controller concerned together: a lack of cooperation between the authorities would result in the data controller being left in limbo. Not only may the incident response be hampered, he may also be exposed to fines under one regime for non-comliance.

The dilemma may even be worse, 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. Hence, one incident would be reported under two different regimes, by two different actors, very likely with non-identical yet similar information. With a lack of cooperation and information exchange between the different competent authorities, the incident may not be identified as one single incident, and thus, even be treated differently with early disclosure very likely. If cooperation does not become mandatory in such scenarios, coherence could only be achieved by implementing a joint reporting scheme. Ultimately, it is up to the national legislators to introduce cooperation mechanisms and requirements for security incidents in which personal data are compromised. These mechanisms need to be based on a certain level of liaison competence in all relevant authorities.

[23] See Art. 13(3) Police Directive.

4 Conclusion and Lessons Learned

Privacy and security in information technology of vital infrastructures are intertwined concepts where incidents in one domain most often have effects in the other. Moreover, the core technology to protect both are the same and need to achieve the same three core protection goals: confidentiality, integrity and availability. It is important to emphasise that in no case any of these three core goals can be omitted.

However, privacy and IT security do differ substantially when considering which assets need to be protected form which kind of threat and attacker: while privacy often boils down to confidentiality of certain types of data (personal information or metadata of usage at foremost), IT security, especially in the context of vital infrastructures, often focuses on the integrity of operational data and the availability of the service.

The above difference is reflected in the legal framework and has effects of the incident reporting obligations in the GDPR and NIS Directive. In particular, we observe variance in when to inform and who to inform. This differences can lead to tricky situations if reporting duties in both frameworks concern the same technical incident. Since neither of the legal instruments supersedes the other, there is no defined processing order. Security and privacy teams need to decide on a case by case basis how to report incidents in a coordinated fashion. A legal obligation of this coordination is currently missing but would be desirable.

While coordination on premise of the service provider / data processor can be expected without new policy, the cooperation of the competent authorities might lack behind expectations. Currently, a general willingness to cooperate might be expressed, but there is no detailed legal obligation nor evidence for a systematic approach to cooperation. Moreover, the different cultures and expertise in the data protection and incident response communities make a coordinated approach to joint incidents harder. Here mutual education is needed.

Failing in cooperation might have a negative impact on the goals of both sides: On the one hand, informing the general public about incidents prematurely, might tip off criminals that run the attack helping them to either destroy evidence or adopt the attack. On the other hand, informing victims for a privacy breach too late might leave their assets at risk for longer than necessary. Hence, optimal timing needs to consider to the inner workings of the attack and the assets of all stakeholders at risk.

While handling security and privacy incidents, the general advice should be: Lawyers: find a tech-geek for help; Computer Scientists: find a law-buff for help.

References

1. Sandra Schmitz and Stefan Schiffner. Don't tell them now (or at all) – end user notification duties under GDPR and NIS Directive. Manuscript submitted for publication, 2021.

2. Marit Hansen, Meiko Jensen, and Martin Rost. Protection goals for privacy engineering. In *2015 IEEE Security and Privacy Workshops*, pages 159–166. IEEE, 2015.
3. M. Martini. Art. 33 DSGVO. In B. Paal and D. Pauly, editors, *Beck'sche Kompakt-Kommentare, Datenschutz-Grundverordnung Bundesdatenschutzgesetz*. C.H. Beck, München, 2018.
4. WP Art 29. Guidelines on personal data breach notification under Regulation 2016/679, WP250 rev.01. 2018.
5. D. Uwer. § 29 BDSG. In S. Brink and H.A. Wolff, editors, *Beck'sche Beck'scher Online-Kommentar Datenschutzrecht*. C.H. Beck, München, 2018.
6. WP Art 29. Guidelines for identifying a controller or processor's lead supervisory authority, WP 244 rev.01. 2017.
7. P. Cichonski, T. Millar, T. Grance, and K. Scarfone. Revision 2: Computer security incident handling guide recommendations. *NIST Special Publication 800-61*, 2012.
8. P. Laue. Art. 34 DSGVO. In G. Spindler and F. Schuster, editors, *Recht der elektronischen Medien*. C.H. Beck, München, 2019.